NAVAL POSTGRADUATE SCHOOL
Monterey, California

THESIS

THE IMPACT OF THE DEFENSE DATA NETWORK ON NAVAL COMMUNICATIONS DURING THE 1980S

by

Victor Bernard Stuckey

March 1988

Thesis Advisor: Judith Lind

Approved for public release; distribution is unlimited

REPORT DOCUMENTATION PAGE

1a REPORT SECURITY CLASSIFICATION UNCLASSIFIED	1b RESTRICTIVE MARKINGS
2a SECURITY CLASSIFICATION AUTHORITY	3 DISTRIBUTION / AVAILABILITY OF REPORT Approved for public release; distribution is unlimited.
2b DECLASSIFICATION / DOWNGRADING SCHEDULE	
4 PERFORMING ORGANIZATION REPORT NUMBER(S)	5 MONITORING ORGANIZATION REPORT NUMBER(S)
6a NAME OF PERFORMING ORGANIZATION Naval Postgraduate School 6b OFFICE SYMBOL (*If applicable*) 62	7a NAME OF MONITORING ORGANIZATION Naval Postgraduate School
6c. ADDRESS (*City, State, and ZIP Code*) Monterey, California 93943-5000	7b. ADDRESS (*City, State, and ZIP Code*) Monterey, California 93943-5000
8a NAME OF FUNDING / SPONSORING ORGANIZATION 8b OFFICE SYMBOL (*If applicable*)	9 PROCUREMENT INSTRUMENT IDENTIFICATION NUMBER
8c. ADDRESS (*City, State, and ZIP Code*)	10 SOURCE OF FUNDING NUMBERS PROGRAM ELEMENT NO / PROJECT NO / TASK NO / WORK UNIT ACCESSION NO

11 TITLE (*Include Security Classification*) THE IMPACT OF THE DEFENSE DATA NETWORK ON NAVAL COMMUNICATIONS DURING THE 1980S

12. PERSONAL AUTHOR(S)
STUCKEY, Victor Bernard

13a. TYPE OF REPORT	13b TIME COVERED	14 DATE OF REPORT (*Year, Month, Day*)	15 PAGE COUNT
Master's Thesis	FROM _____ TO _____	March 1988	86

16. SUPPLEMENTARY NOTATION The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government.

17 COSATI CODES			18 SUBJECT TERMS (*Continue on reverse if necessary and identify by block number*)
FIELD	GROUP	SUB-GROUP	Defense Data Network, DDN, Navy Implementation

19 ABSTRACT (*Continue on reverse if necessary and identify by block number*)

The Defense Data Network (DDN) is a packet-switchng network that provides data transport services to the Department of Defense. The primary focus of this thesis is to assess the DDN's impact upon Naval communications

The Navy's implementation plan for the transition to the DDN is described. Benefits for Navy subscribers and problem areas associated with the DDN program implemention are discussed. Recommendations are presented that can improve the transition process for future DDN subscribers and alleviate many present-day problems.

This study concludes that the DDN has had minimal impact on Naval communications until now. In order to improve the DDN's acceptability among Navy subscribers and to avoid unnecessary problems in the future, more

20 DISTRIBUTION / AVAILABILITY OF ABSTRACT ☒ UNCLASSIFIED/UNLIMITED ☐ SAME AS RPT ☐ DTIC USERS	21 ABSTRACT SECURITY CLASSIFICATION UNCLASSIFIED
22a NAME OF RESPONSIBLE INDIVIDUAL Judith Lind	22b TELEPHONE (*Include Area Code*) (408) 646-2594 22c OFFICE SYMBOL 55Li

19. Abstract continued.

command-level attention must be focused on the Navy's DDN program. Continuous interaction and dialogue must be maintained between established Navy DDN subscribers and potential subscribers.

Approved for public release; distribution is unlimited.

THE IMPACT OF THE DEFENSE DATA NETWORK ON NAVAL COMMUNICATIONS DURING THE 1980s

by

Victor Bernard Stuckey
Lieutenant, United States Navy
B.S., Savannah State College, Savannah, Georgia, 1979

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF SCIENCE IN TELECOMMUNICATIONS
SYSTEMS MANAGEMENT

from the

NAVAL POSTGRADUATE SCHOOL
March 1988

ABSTRACT

The Defense Data Network (DDN) is a packet-switching network that provides data transport services to the Department of Defense. The primary focus of this thesis is to assess the DDN's impact upon Naval communications.

The Navy's implementation plan for the transition to the DDN is described. Benefits for Navy subscribers and problem areas associated with the DDN program implementation are discussed. Recommendations are presented that can improve the transition process for future DDN subscribers and alleviate many present-day problems.

This study concludes that the DDN has had minimal impact on Naval communications until now. In order to improve the DDN's acceptability among Navy subscribers and to avoid unnecessary problems in the future, more command-level attention must be focused on the Navy's DDN program. Continuous interaction and dialogue must be maintained between established Navy DDN subscribers and potential subscribers.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

ACKNOWLEDGEMENTS

The author acknowledges the contributions and professional guidance of Professors Judith Lind and Dan Boger and Commander John Donnelly, USN. In addition, the author acknowledges the invaluable assistance of Mrs. Margaret Campbell for the expertise and patience exhibited in her role as the thesis typist. Special thanks to Mrs. Dorothy Stuckey (the author's mother) for her undying love and support. This thesis is dedicated to the memory of Mr. Charlie Stuckey (the author's father).

I. INTRODUCTION

A. PURPOSE

The Defense Data Network (DDN) is a Department of Defense (DOD) approach to providing rational, standard, and interoperable data communications services, mandated for all defense agencies [Ref. 1:p. 22]. This study examines how well the DDN is being utilized by the Department of the Navy (DON) and provides suggestions concerning how that utilization can be improved and enhanced.

The research for this thesis is geared toward answering the following questions:

1. How effectively is the Navy utilizing the DDN System for daily, routine message traffic?
2. What could be done to increase the acceptability and usage of the DDN throughout the DON?
3. What advantages and disadvantages does the DDN present to the Navy?

B. BACKGROUND

In 1980 the AUTODIN II DOD communication system failed to meet its extended initial operational capacity target, thus prompting the Assistant Secretary of Defense for Command, Control, Communications, and Intelligence to order a review of possible alternatives to the AUTODIN II program [Ref. 2:p.7]. In September 1981 lingering doubts regarding technical performance and survivability led the Defense

Communications Agency (DCA) to establish two separate design teams to develop the most survivable AUTODIN II system and also an alternative system based on existing ARPANET communication technology.

The ARPANET is a packet-switched data communications network developed by the Defense Advanced Research Projects Agency (DARPA). ARPANET was developed purely as an experimental network chartered to advance the state of the art in computer resource sharing. It was designed to provide efficient communications between heterogeneous computers so that hardware, software, and data resources could be shared conveniently and economically by a wide community of users. As the initial research and development goals of the network were attained, users with operational requirements in addition to those with experimental requirements began to use the ARPANET.

Subsequent reviews of the three design teams' reports, coupled with a review by a Defense Science Board task force, led to the conclusion that the ARPANET system better fit DOD needs for data communications than did the others. On 2 April 1982 the AUTODIN II program was terminated and the Deputy Secretary of Defense directed the implementation of the DDN [Ref. 2: p. 7].

The 1982 DDN Program Plan called for the creation of a single packet-switching network. The network would consist of 171 packet switches located at 85 geographical sites and

would provide service for 488 host computers and 1446 terminals. The network was to be comprehensive, serving all security levels using end-to-end encryption devices. The newly formed DDN system included three segments. The ARPANET consisted of approximately 100 packet switches and served both the networking research community and the unclassified communications requirements of DOD users. The Movements Information Network (MINET) was in the process of being installed. It was to consist of 12 packet switches and was intended to serve the logistics community of the U. S. forces in Europe. The Worldwide Intercomputer Network (WIN or WINCS) consisted of 17 packet switches and provided long-haul data transport for the Worldwide Military Command and Control System (WWMCCS). The WIN was the only DDN segment handling classified traffic [Ref. 2:p. 9].

In 1983 the original ARPANET system was divided into two segments. ARPANET, consisting of 40 packet switches and 53 trunks, was continued as a network serving the networking research community. The Military Network (MILNET), consisting of 57 switches and 89 trunks, became the major DDN segment for the transport of unclassified data. In 1984 the MINET system was absorbed into the MILNET, thereby creating a single unclassified segment named the MILNET, serving operational military users. By October 1985 the MILNET consisted of 100 packet switches worldwide, supported over

300 operational hosts, and passed more than 14 million packets per day. [Ref. 2:pp. 9-10]

Providing a more survivable backbone communications capability than AUTODIN II, the DDN is designed to incorporate the maximum practical modularity and flexibility in the backbone system and its various interfaces to accommodate significant changes in user requirements, in automatic data processing (ADP) and data communications technology, and in economic factors. In March 1983 the Under Secretary of Defense for Research and Engineering stated:

> All DOD ADP systems and data networks requiring data communications services will be provided long-haul and area communications, interconnectivity, and the capability for interoperability by the DDN. Existing systems, systems being expanded and upgraded, and new ADP systems or data networks will become DDN subscribers. [Ref. 3:p. 4]

The concept of the DDN is that of a multilevel secure communications network. At the present time the operational and planned subnetworks of the DDN include:

1. ARPANET - Experimental network
2. MILNET - Unclassified segment
3. DISNET - Defense Integrated Secure Network
4. SACDIN - Strategic Air Command Digital Network
5. SCINET - Sensitive Compartmented Information Network
6. WIN/WINCS - WWMCCS Intercomputer Network. [Ref. 4:p. 9]

Figure 1.1 depicts the planned evolution of the DDN. DISNET, SACDIN, SCINET, and WIN eventually are to integrate

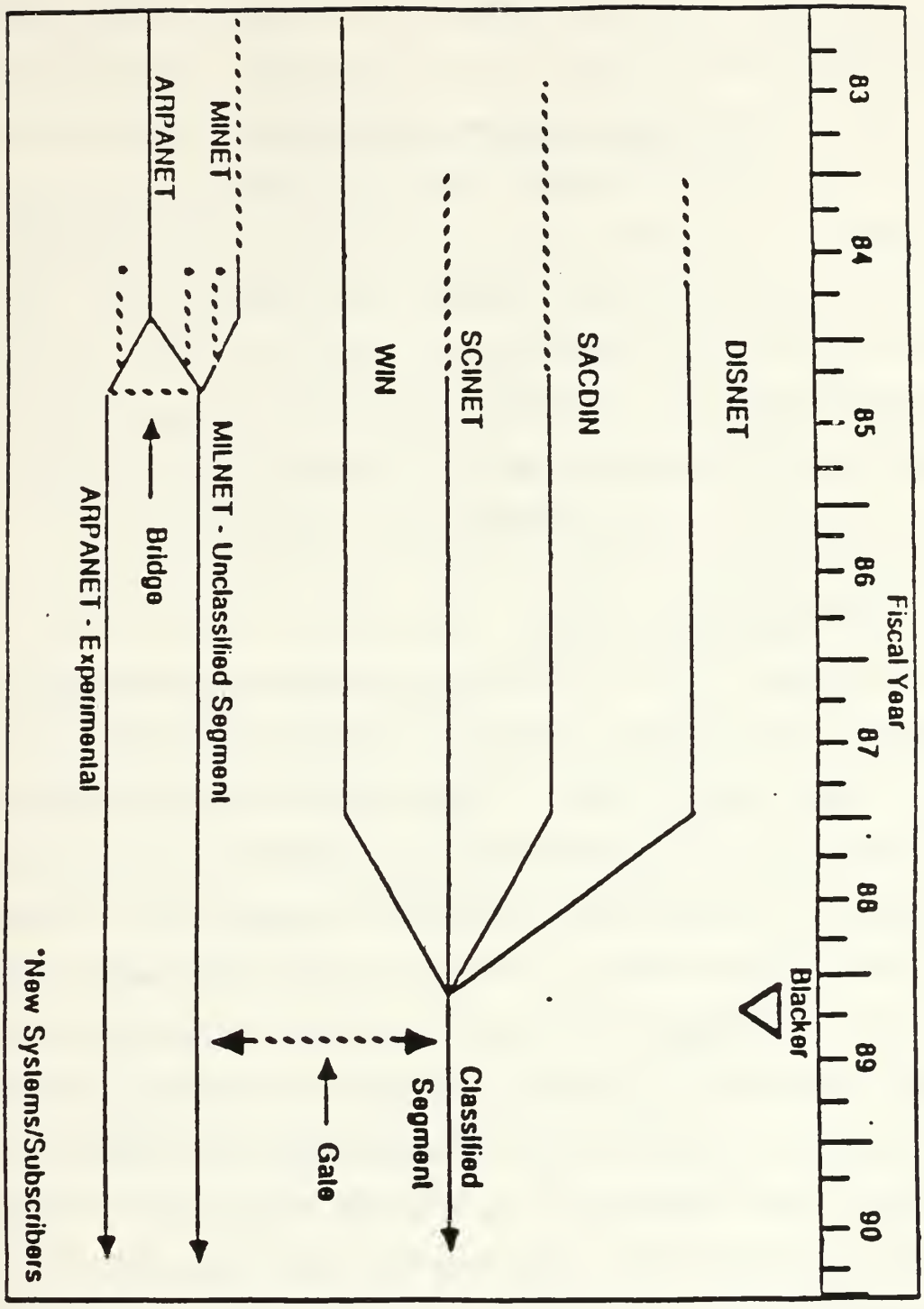

Figure 1.1 Planned Evolution of DDN.
[from Ref. 5:p. 5-2a]

to form the classified segment of the DDN, interconnecting via one-way switch-level network gateways. The final phase in the integration of the classified data subnetworks revolves around a National Security Agency device called BLACKER. The BLACKER device will permit the segmented DDN to evolve into a single, shared, multilevel secure network. The Inter-Service/Agency Automatic Message Processing Exchange subnetwork and other multilevel secure hosts will also be able to use the DDN as a backbone as a result of the availability of BLACKER technology. [Ref. 4:p. 3]

C. ORGANIZATION OF THESIS

Chapter I of this thesis provides a historical perspective for the DDN, including background information on the origin of the DDN. Packet-switching technology, DDN architecture and components, and system protocols are discussed in Chapter II. Chapter III examines the uses of the DDN as they relate to communications throughout the DOD. The fourth chapter describes the funding of the DDN and how Usage Sensitive Billing will be used for future DDN costs. In Chapter V future DDN capacity and requirements are analyzed with respect to the DDN user population, limits to growth, technological improvements, and the ability of the DDN to accommodate changes in user requirements. Chapter VI describes the DON's implementation plan and gives the strengths and weaknesses of the plan, along with an assessment of the plan. Finally, Chapter VII presents the conclusions and recommendations of this thesis.

II. DEFENSE DATA NETWORK TECHNOLOGY

A. PACKET-SWITCHING TECHNOLOGY

The key distinguishing feature of a packet-switched system is that a computer organizes outgoing digital information into individual segments. The segments are called packets. The structure of a typical packet includes (1) header information, (2) a header error check, (3) the data, and (4) a data error check. Packet switching begins after the digital information source associated with the user terminal has produced enough bits to fill the data bits field. The host computer then attaches a carefully formatted block of header items. Packets make their way independently to receiving stations where other computers reassemble the segments into replicas of the original message. [Ref. 6:p. 9]

Many objectives are served by this technique. Perhaps the most important is increased efficiency in the utilization of expensive transmission facilities such as satellite frequency bands or long-haul terrestrial links. This objective is accomplished by filling in all the natural time gaps between blocks of information on the channel. Another objective achieved by packet-switched systems is robustness with respect to blockage on particular links in the network. An additional system objective which is closely related is

assurance of the accuracy of all the bits in a received message. [Ref. 7:p. 24]

1. Packet-Switched Network Component

The components of a basic packet-switched network include user terminals, host computers, and network or switching nodes. User terminals can take a variety of forms, including a teletype keyboard and printer, an interactive data and graphics cathode ray tube (CRT) terminal, a telephone handset and associated digital interface, or a software process in a computer. A CRT terminal can even represent an entire independent local network joining multiple user facilities.

The host computer provides the user terminals attached to it with all of the services and translations needed to get their data to and from the network. The host will provide packetizing and depacketizing service for "dumb" terminals and lesser services for "intelligent" terminals or networks.

Host computers are joined to the network nodes via some type of transmission media. These nodes consist of relatively powerful switching and routing control computers which receive, sort, store, and forward packets to the network. These computers use route selection algorithms which accommodate network conditions and performance objectives. Each node is linked to several other nodes via various types of transmission media and provides several

different routes for data to flow between users of the system. Each packet received at an intermediate node typically is stored in a buffer queue until processing capacity is available to decide what to do with the packet. Once the packet is at the head of the queue, the processor examines the packet for its destination address, decides what node to send it to next, and places the packet in a queue awaiting transmission via a particular link.

All necessary packet-switching transactions within and between terminal hosts and the network are governed by defined sets of rules called protocols. Protocols provide the participants with a standardized vocabulary of message exchanges and responses needed:

1. To initiate a communication session with a destination.
2. To request and receive transmission capacity.
3. To format, transmit, and acknowledge packets.
4. To terminate the session. [Ref. 6:p. 21]

2. Routing Techniques

In large, highly connected packet networks there are many possible paths between a source and destination. Tremendous amounts of research have been devoted to finding the best path between two points in a network, where best can be defined as minimum length, minimum delay, least cost, least number of hops, maximum flow rate, or some combination of these. Each node has a degree of independence in choosing the next node in order to achieve the best path in

the end-to-end sense. Various adaptive techniques have been used to permit nodal processors to account for large scale network conditions such as regions of temporary congestion or link outages in order to try to improve the end-to-end quality of paths.

Often a fixed or static routing table is used where each source-destination pair is evaluated and a best path is developed and placed in a table. In this way, when an intermediate node notes a packet's destination, it merely checks the table and sends the packet on toward the designated node. This appears to be simple but, due to the growth of large networks, changes to links and nodes occurring more frequently, and to instances of temporary congestion, the result is frequently poor performance in packet delivery [Ref. 8:p. 115]. Because of this, almost all long-haul packet-switched networks use some sort of dynamic routing algorithm which bases the routing decision on measurements, or estimates, of the current traffic and topology of the network. Table I lists the recognized requirements for packet-switched networks [Ref. 9:p. 12].

The DDN uses a routing strategy known as adaptive directory source routing [Ref. 8:p. 121]. Each node sends a packet to all other nodes every 10 seconds, called a Link State Packet. This packet contains information about the state of a node's links with all its neighbor nodes in terms of delay for a packet to be sent along that link. A simple

TABLE I

PACKET-SWITCHED NETWORK ROUTING REQUIREMENTS
[From Ref. 9:p. 12]

Message routing should ensure rapid and error free packet delivery
Routing strategy should adapt to changes in network topology resulting from node and communication link failures
Routing techniques should adapt to varying source/ destination traffic loads
Packets should be routed around congested or blocked nodes
Packets should be routed to their destination via some least-cost method
A technique for detecting looping and "ping-ponging" should be included
Routing techniques should be as simple as possible to minimize hardware and software requirements

but elegant broadcasting technique known as intelligent flooding ensures that all nodes receive the link status packet. Upon receipt of each new link status packet, the node develops a new routing table for sending normal packets traversing the network. This table generation requires an efficient but complete database that enables each node to have a complete map of the network. The table must maintain consistent network mapping from node to node. [Ref. 10:p. 93]

3. Packet-Switched Network Advantages

Packet switching is particularly well suited to military data communications and was developed specifically for computer communications. It can support the real-time communications required by computer systems and can provide the high levels of circuit utilization required by cost-conscious system designers and managers. Furthermore, because packet-switching nodes (PSNs) typically can operate without an attendant, and because they are small, reliable, and inexpensive, they can be installed in large quantities and at many locations, thus providing substantial survivability. [Ref. 9:p. 22]

B. DDN PROTOCOL SUITE

The design, development, and standardization of packet system protocols have received a great deal of attention. Protocols exist to ensure that communicating entities can send, receive, and interpret the information that they wish to exchange. Protocols play three fundamental roles:

1. They establish standard data elements.
2. They establish conventions.
3. They establish standard communication paths.

Data elements include characters, messages, files, jobs, and graphic displays. Conventions include code sets, packet formats, transmission speeds, and control messages. Standard communication paths can include functions such as addressing, priority setting, sequencing, error control,

flow control, and session initiation and termination. [Ref. 7:p. 29]

1. Network Access Protocol

Within the DDN, network access is via the ARPANET 1822 protocol or the DDN X.25 protocol. The DDN currently supports both protocols as coequals, but will eventually phase out the 1822 protocol. [Ref. 11:p. 5-1]

The 1822 protocol is an asynchronous, bit-serial interface that provides physical and data link services over distances of less than 2000 feet between a subscriber device and a PSN. Four variations of the 1822 protocol include:

1. Local host
2. Distant host
3. Very distant host
4. High-level data link control distant host (HDH). [Ref. 11:p. 5-2]

The DDN X.25 protocol provides two types of service, basic and standard. Basic service is equivalent to the International Telegraph and Telephone Consultative Committee recommendation X.25 protocol. This protocol is oriented toward hosts that have existing higher-level protocol implementations that require reliable delivery of packets. Standard service is oriented toward hosts using DOD standard higher-level protocols. The DDN will provide interoperability between the 1822 and the X.25 service. Only basic X.25 service and 1822 protocols are currently supported by the DDN [Ref. 11:p. 5-1]. The interoperability features of

DDN basic X.25, DDN standard X.25, and 1822 protocols are shown in Table II. [Ref. 5:p. 8-8a]

2. Internet Protocol (IP)

The IP interconnects networks with various internal protocols and performance parameters with minimal impact on each network. IP defines the format of internet packets and the rules for protocol functions based on control information in the packet header. This protocol supports the delivery of datagrams from source to destination nodes. A datagram is a self-contained packet, independent of other packets, that does not require acknowledgement and carries sufficient information for routing from the originating data terminal equipment without relying on earlier exchanges between the terminal equipment and the network. [Ref. 5:p. 8-10]

A generalized set of parameters is used to select characteristics for transmission through each network. These parameters require trade offs between low delay, high reliability, and high throughput. IP utilizes four levels of precedence that are used by the DDN to measure the importance of a datagram. These precedence levels include:

1. Flash: response required in less than 10 minutes.
2. Immediate: response required in less than 30 minutes.
3. Priority: response required in less than three hours.
4. Routine: response required in less that six hours.

An example of communication flow using IP is depicted in Figure 2.1.

TABLE II

INTEROPERABILITY FEATURES OF DDN BASIC X.25, STANDARD X.25, AND 1822 PROTOCOLS
[From Ref. 5:p. 8-8A]

	DDN Basic X.25	DDN Standard X.25	1822 HDH
Requires TCP/IP		x	x
Requires vendor ULP	x		
Supports HDLC at link level	x	x	x
Communicates with 1822 HDH hosts		x	x
Supports homogeneous hosts	x	x	x
Supports heterogeneous hosts		x	x
Communicates across DDN gateways		x	x
Reliability provided by transport protocol		x	x
Compatible with International Standard	x		
Provides for DDN terminal-to-host communication		x	x
Communicates with basic X.25 hosts	x		
Supports BLACKER devices		x	

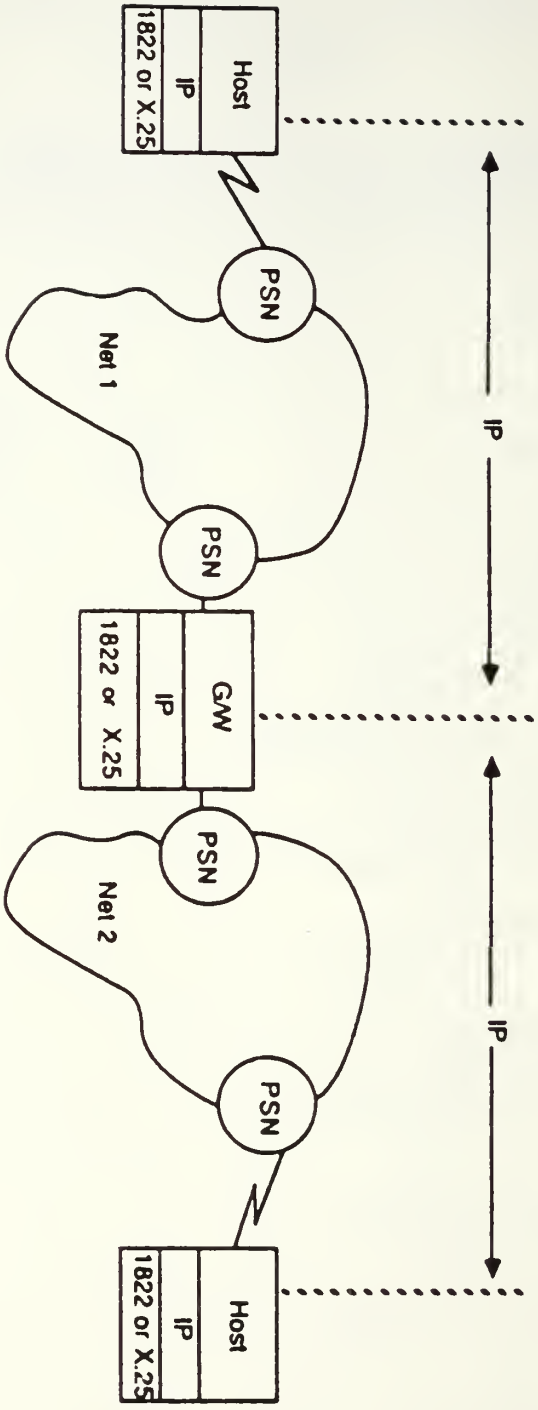

Figure 2.1 Communication Flow Using IP.
[from Ref. 5:p. 8-10a]

3. Internet Control Message Protocol (ICMP)

The ICMP must be implemented in every IP module. It is used by a gateway or destination host to notify a source host of error conditions. ICMP uses the basic support of IP, including IP headers, as if it were a higher level protocol, but it is actually an integral part of IP implementation. This relationship is illustrated in Figure 2.2. ICMP is designed to supply feedback about problems in network communications, but it is not designed to make IP more reliable [Ref. 11:p. 8-14]. ICMP messages are sent when:

1. A datagram cannot reach its destination.
2. A gateway does not have buffering capacity to forward a datagram.
3. A gateway can direct the host to send traffic on a shorter route. [Ref. 5:p. 8-14]

4. Transmission Control Protocol (TCP)

TCP was developed to replace the earlier Network Control Protocol that allowed applications software to send messages throughout the network with a minimum of protocol mechanisms (see Figure 2.3). TCP provides the following functions:

1. Establishes and maintains interprocess communications.
2. Maintains reliable communications by providing eight-bit word sequencing and accounting.
3. Controls the flow of data transferred between the sender and receiver systems.
4. Multiplexes several processes within a single host so they may communicate simultaneously using TCP.

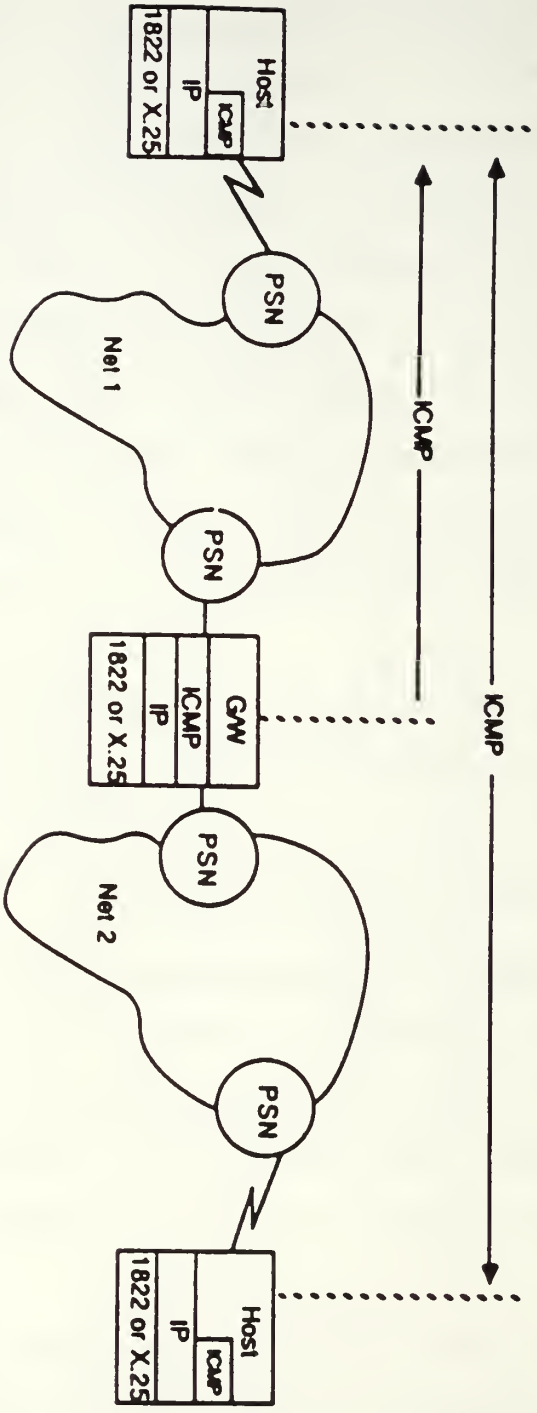

Figure 2.2 Communication Flow Using ICMP
[from Ref. 5:p. 8-14a]

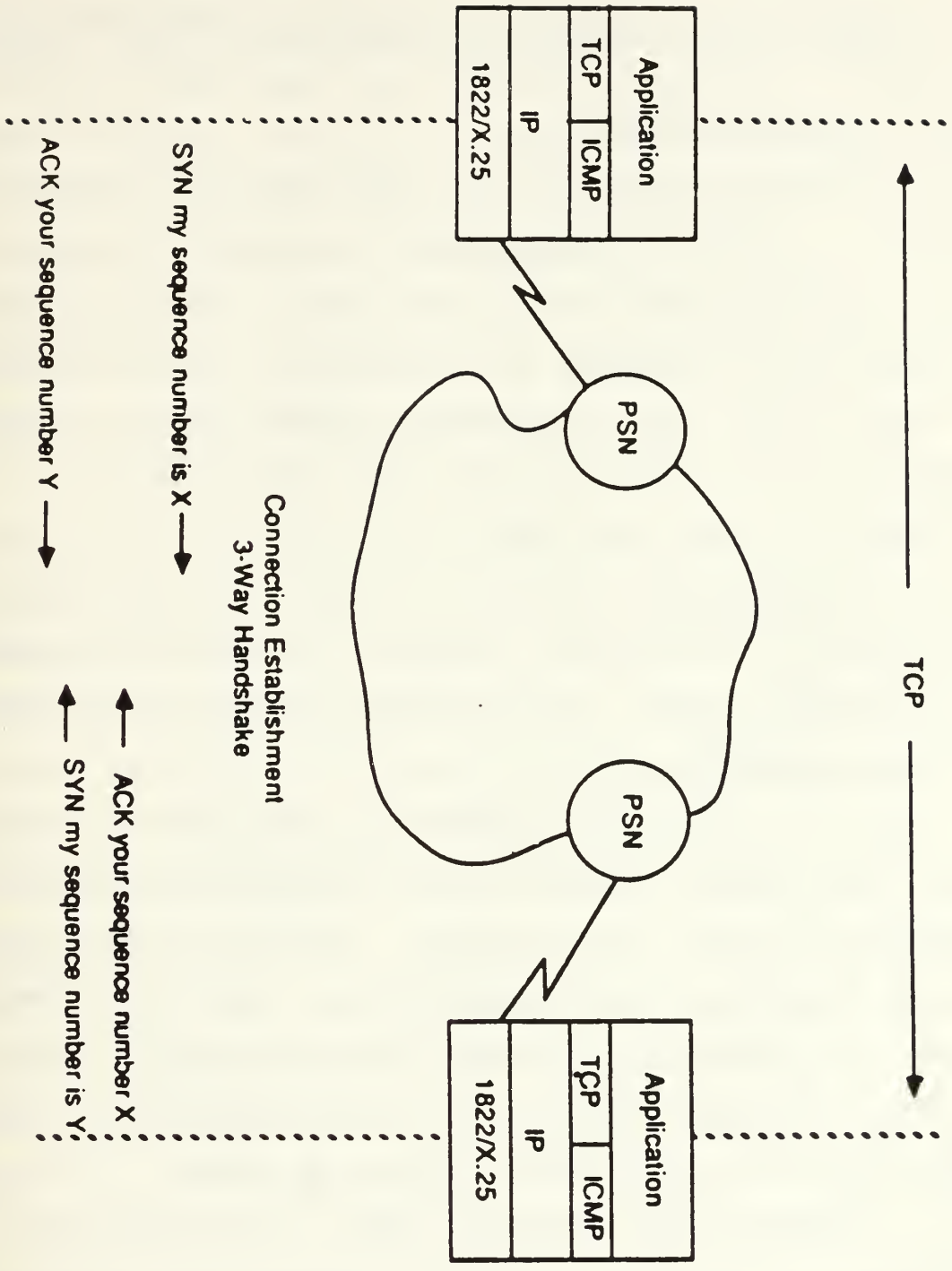

Figure 2.3 Communication Flow Using TCP.
[from Ref. 5:p. 8-16]

5. Generates a level of priority and security for communications being undertaken by the TCP. [Ref. 5:p. 8-15]

5. Gateway Protocols

Gateway protocols enable communications between DOD networks. These protocols allow computers to act as loosely-coupled packet-switching communications systems. Multiple sets of gateways can implement a composite single internet system, but homogeneous gateways under a single authority and control are best for maintainability and operability. [Ref. 5:p. 8-27]

An autonomous system consists of a set of one or more relatively homogeneous gateways. An internet is a set of autonomous systems. One internet consists of the DARPA gateways on ARPANET.

A stub gateway interfaces a local network to the rest of the internet and only handles traffic originating or terminating on the local network. Interior neighbors are part of the same autonomous system (i.e., two core gateways on the same network). Exterior neighbors are not part of the same autonomous system (i.e., a stub gateway and a core gateway that share a network). [Ref. 5:p. 8-28]

Gateway-gateway protocol (GGP) is used with the IP to determine whether network interfaces and neighbor gateways are operational and connectivity is possible. The gateway sends itself "interface probe" packets every 15 seconds to make sure it is still operational and sends

"neighbor probe" packets to operational neighbors every 15 seconds to make sure they are still operational. Routing-update messages are sent to neighbor gateways when a change occurs in internet routing. Routing-update messages indicate the distance and address of the gateway on the shortest path to the network. If a gateway goes down, packets will be rerouted via an alternate gateway without disrupting host-to-host connections. [Ref. 5:p. 8-29]

Exterior gateway protocol (EGP) conveys network reachability information between neighboring gateways outside the core system. EGP has mechanisms to acquire neighbors, to monitor neighbor reachability, to exchange update messages, and to allow gateway systems to pass routing information to internet gateways. Subscribers are permitted to perceive all network and gateways as part of one internal system even though exterior gateways may use a routing algorithm not compatible with interior gateways. Periodic polling "hello/I heard you" messages monitor neighbor reachability and solicit update information. Each stub gateway has a list of networks reachable via that gateway, including the number of hops. Gateway lists include gateways directly connected to the network specified in the IP source network field of the last received poll command. Figure 2.4 gives a basic representation of how the DDN gateways interface. [Ref. 5:p. 8-31]

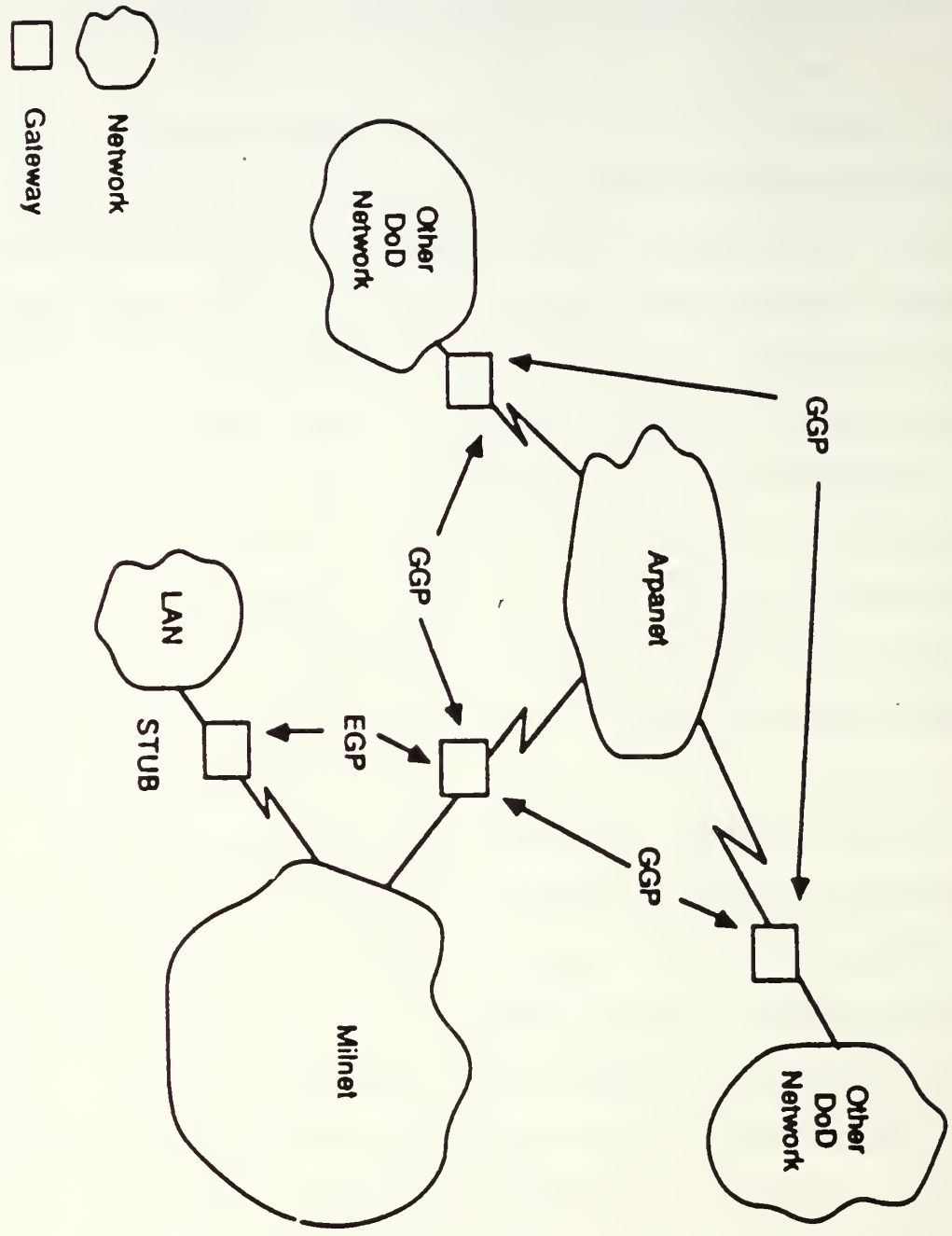

Figure 2.4 Gateways Connecting DDN Components
[from Ref. 5:p. 8-27a]

C. DDN ARCHITECTURE

The DDN is an integrated packet-switching network composed of two functional areas: a backbone network and an access network (see Figure 2.5). The backbone network is composed of PSNs and high speed interswitch trunk circuits that connect the packet switches. PSNs support only host interfaces, and therefore anything connected to a PSN must look like a host.

An access network is composed of leased circuits, dial-up circuits, and equipment necessary to connect host computers and terminals to the PSNs and the backbone network. Access networks provide two top level network-wide functions: safeguarding the security and privacy of subscriber traffic, and monitoring and controlling network performance. [Ref. 11:p. 5-4]

1. Backbone Network

The DDN backbone has grown to be a highly survivable network of several hundred packet switches located at the DDN PSNs throughout the world. Each packet switch is a Bolt, Beranek and Newman (BBN) C/30 microprogrammed minicomputer. The C/30 is a current generation computer designed for unattended operation, easy maintenance, and compatibility with existing ARPANET packet-switching software. It provides the DDN with high reliability through redundancy, self monitoring capability, graceful performance degradation (versus catastrophic failure), and automatic program reload capability. [Ref. 4:p. 4]

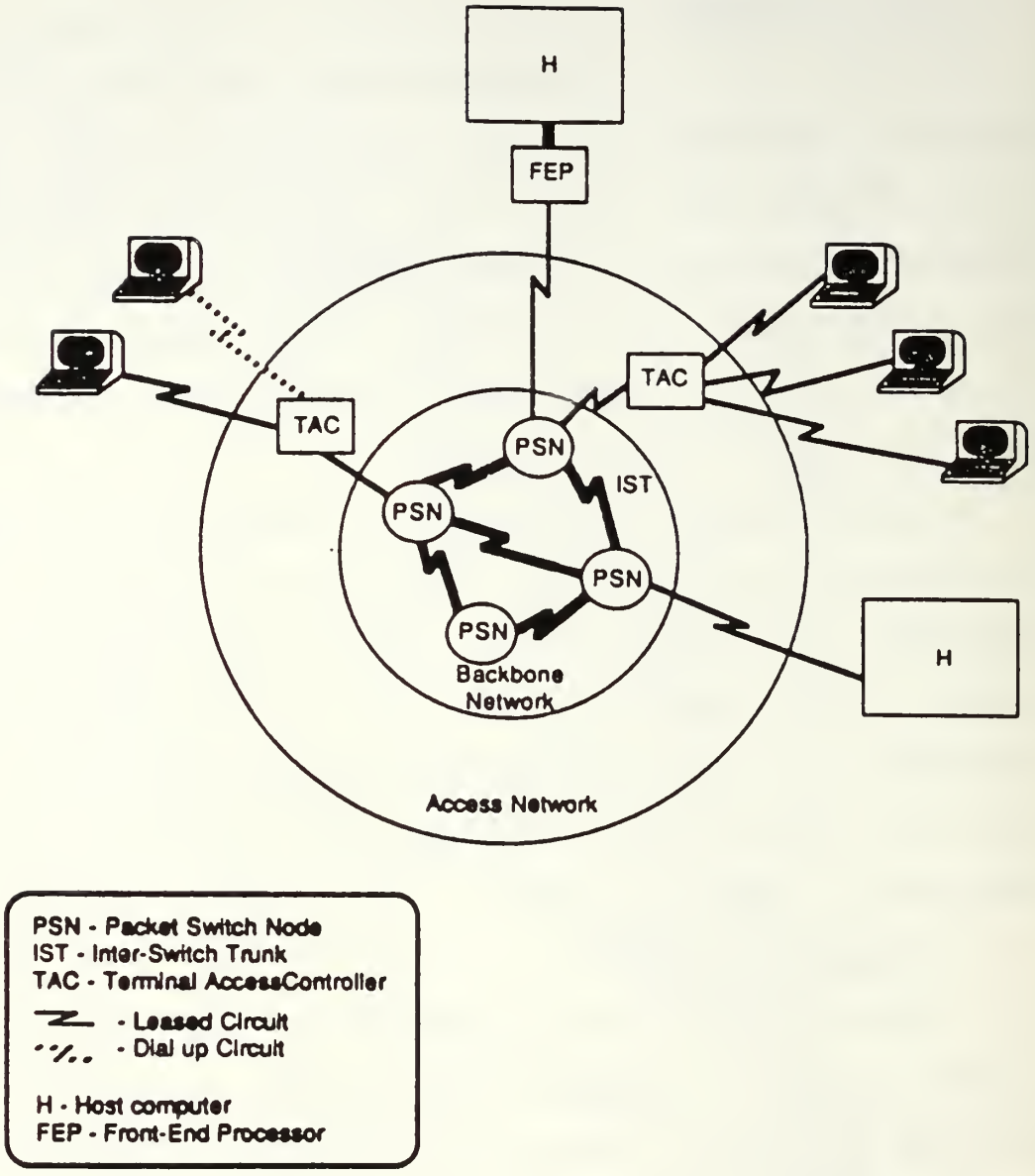

Figure 2.5 Basic DDN Architecture.
[from Ref. 5:p. 5-17a]

Most of the backbone transmission links are terrestrial, leased circuits. They generally are either digital circuits operating at 56,000 bits per second (bps), or analog circuits operating at 48,000 bps overseas and 50,000 bps in the continental United States. Transoceanic links are via satellite and submarine cable. [Ref. 4:p. 3]

2. Access Network

Host computer systems are connected to the DDN packet switches through DDN-developed host front-end processors (HFEP), terminal emulation processors (TEP), or directly via X.25 or 1822 protocol interfaces. The transmission speeds of the host circuits are 2400 to 56,000 bps. Each host system can be directly connected to one or more packet switches by one or more circuits. [Ref. 4:p. 5]

Individual terminal users are connected to the network either through a Terminal Access Controller (TAC) or indirectly through a host which is directly connected to the network. A TAC provides a method for asynchronous terminals to access the backbone network. Each TAC can support up to 64 terminals connected to it with either leased or dial-up lines operating at speeds ranging from 100 to 19,200 bps. Each of the TACs is connected to a packet switch in the network backbone via a leased line operating at 4800 to 56,000 bps. TACs are described in more detail in a later section. [Ref. 5:p. 5-17]

3. DDN Architectural Features Related to Security

The DDN is composed of two backbone network segments for security reasons: a classified segment, and an unclassified segment. The microprocessor-based Internet Private Line Interface (IPLI) provides end-to-end encryption in the classified segment by cryptographically separating the traffic of each security level or special community. Link encryption in the classified segment and for all transoceanic links is accomplished using KG-84 electronic encryption devices. [Ref. 4:p. 4]

In the unclassified DDN backbone segment, link encryption utilizes standard data encryption devices in the U.S. and KG-84s overseas. A classified source subscriber and classified destination subscriber can communicate across a path that traverses the unclassified segment through the use of switch-level gates or gateways which link the two segments. Unclassified traffic, however, is not allowed to cross the gateways into the classified segment of the DDN. [Ref. 5:p. 7-1]

As an added precaution, packet switches and TACs are located in facilities that are physically secure, and C/30 packet switches and TACs are TEMPEST certified. The DDN presently operates as a fully integrated network. The network will support multi-level secure hosts with a single BLACKER device and access line once the BLACKER equipment and technology become universally available [Ref. 4:p. 3].

The anticipated BLACKER application is depicted in Figure 2.6.

4. DDN Control Technology

Fault diagnosis and software maintenance for the DDN are controlled by network monitoring centers (NMCs). The current design includes a primary NMC with designated alternate MCs, regional MCs in Europe and the Pacific, and MCs for each separately-keyed community of subscribers. Each NMC consists of a BBN C/70 minicomputer and software that originally were developed for the ARPANET monitoring center. The personnel of the NMCs will monitor the status of the network, perform fault isolation and diagnosis, and support software maintenance for the packet switches and TACs [Ref. 5:p. 5-25]. The functions of the DDN NMC are noted in Table III.

The Network Information Center (NIC) is responsible for providing information to users of DOD networks, particularly MILNET and ARPANET. The NIC is funded by the DDN program manager's office.

The NIC can be contacted via electronic mail, commercial telephone, or the U. S. postal service. General reference material provided by the NIC includes:

1. The DDN Directory
2. The DDN Protocol Handbook
3. The DDN New Users Guide
4. DDN Newsletter.

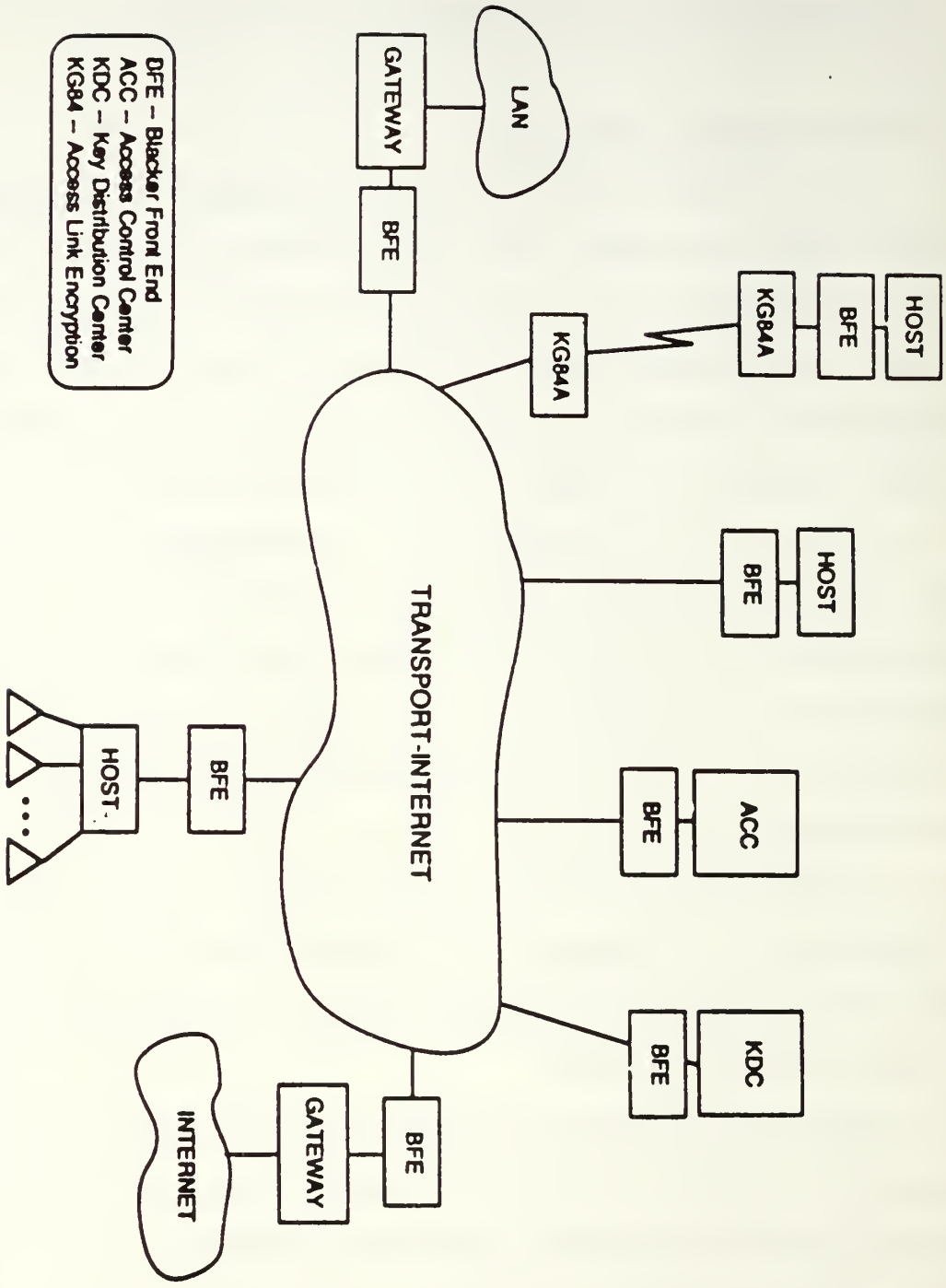

Figure 2.6 Anticipated Typical BLACKER Application for the DDN. [from Ref. 5:p. 7-4a]

TABLE III

NETWORK MONITORING CENTER
FUNCTIONS
[From Ref. 4:p. 30]

1. Assign network resources: since resources must be shared, some networks treat all users equally, while others provide some users privileged access in a priority scheme. This may preempt those currently using resources in order to serve high priority users.

2. Remote switching: the NMC has the ability to load switching software at nodes remotely located from the monitoring centers.

3. Database management: static and dynamic information are updated and maintained on network elements.

4. Adaptive presentation: data can be screened or filtered for special attention and to categorize it for individual users or files.

5. Provide security: secure communication is provided between nodes to avoid spoofing or unintentional network control actions.

6. Establish thresholds: distributed controls may handle problems up to a certain threshold but, once exceeded, the monitoring center may act. Actions may be in the form of establishing additional diagnostic performance monitoring when an unidentified fault is indicated or even providing complete fault detection, isolation, and correction.

Network services provided through the NIC are:

1. NIC/Query program
2. WHO IS
3. TACNEWS
4. NIC Hostname Server.

The NIC also registers MILNET users and assigns TAC access id and passwords for user identification. [Ref. 5:p. 11-14]

D. DDN COMPONENTS/ELEMENTS

1. Packet-Switching Nodes

The PSN (previously called Interface Message Processor or IMP) is the most powerful element of the network. The PSN is a computer-controlled node that:

1. Packetizes messages from local network users and transmits these messages on the network.
2. Routes packets through the DDN by receiving them on the input line, reading their destination, and forwarding them to the node serving the destination host.
3. Reassembles packets into messages for the network user at the destination and forwards these packets to that user.
4. Retransmits packets to a destination node if the previous packet was not acknowledged.
5. Checks packets for transmission errors.
6. Collects performance statistics utilized for packet routing, system analysis, and control. [Ref. 12:p. 15]

The PSN function is performed by an unattended BBN C/30 packet switching processor (discussed in an earlier section). Functionally the PSN provides an almost universal

interface between the multitude of host computers and the network. The PSN's capabilities include:

1. Traffic throughput of 300 packets/second tandem processing (i.e., 300 in, 300 switched, and 300 out simultaneously)

2. Processing delay of under 1 millisecond unloaded, of 1 to 2 milliseconds when moderately loaded, and of 2 to 3 milliseconds when heavily loaded

3. Routing bandwidth and central processing unit overhead of less than 2%, and a reaction to topological or significant delay changes in less than 100 milliseconds. [Ref. 12:p. 16]

2. Terminal Access Controller

The Terminal Interface Processor (TIP) was originally developed for ARPANET to provide network access to a terminal which was not connected directly to a local network host. The TIP was a variation of PSN equipment that provided additional hardware and software to support communications between terminals.

In 1984 the TIP system was replaced by TAC equipment which segmented terminal control and PSN functions into separate components. The TAC is a BBN C/30 computer similar to that used for PSNs, but configured with different software. It is a transmission speed-adaptable component that can provide connectivity to 63 terminals to the network via a PSN. Terminals can access the TAC at bit rates up to 19.2 Kbps. The PSN views the TAC as if it were a host computer for the terminal. The TAC is designed for unattended operation and high reliability. [Ref. 12:p. 17]

3. Terminal Emulation Processor

A TEP is a protocol-interfacing device that attaches to existing terminal ports on a host, providing limited network communications. Terminals on other DDN hosts can access a TEP-configured host through this processor, but local terminals connected to the TEP host cannot access the DDN through such a host. The segregation of host and network responsibilities in terms of communication protocols makes this network access method simple by requiring no host software modifications. The TEP configuration is shown in Figure 2.7. [Ref. 12:p. 18]

4. Host Front End Processor

The preferred technique for interfacing a host with the DDN is through a HFEP protocol-interfacing device. The HFEP is connected to an input/output port on the host system and requires that the host support a common HFEP protocol. Since some host software modifications are required, the resulting system is only as responsive as the host. The HFEP depicted in Figure 2.8 can support bit throughput rates ranging from 4800 bps to 56,000 bps, plus full-duplex operation. [Ref. 12:p. 18]

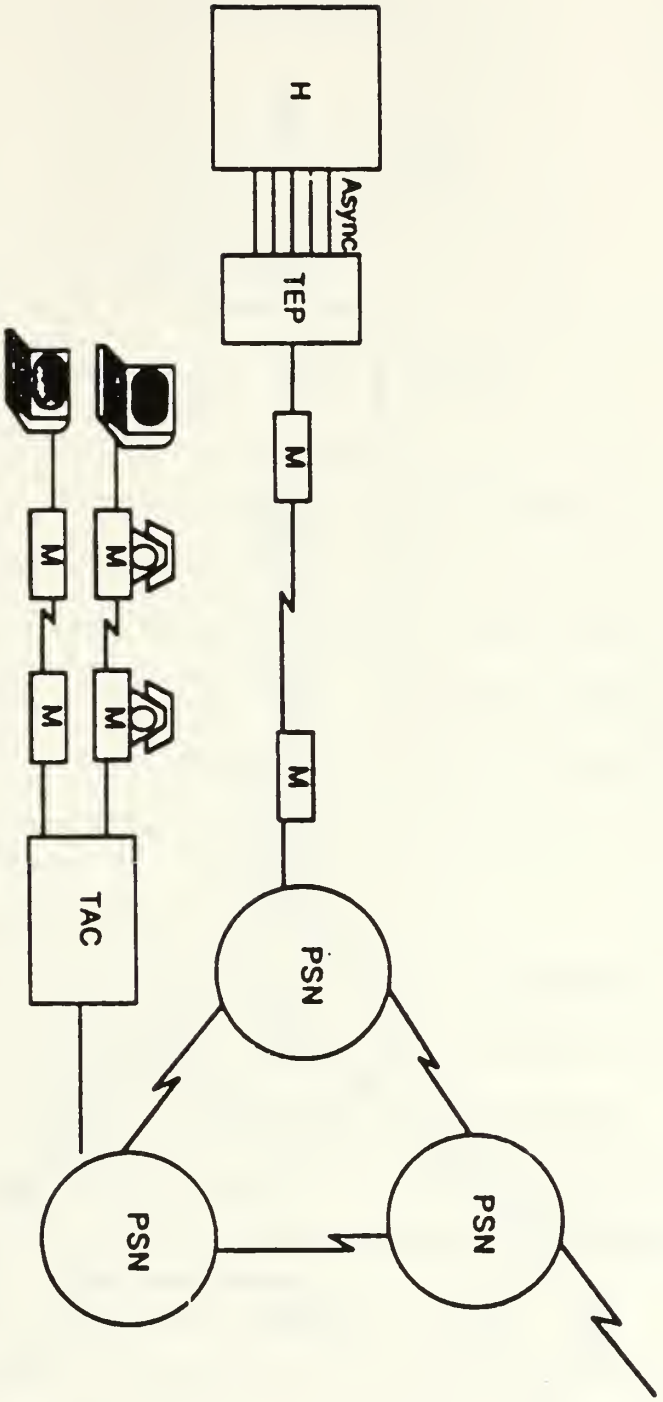

Figure 2.7 Communication Flow Using TEP.
[from Ref. 5:p. 5-21a]

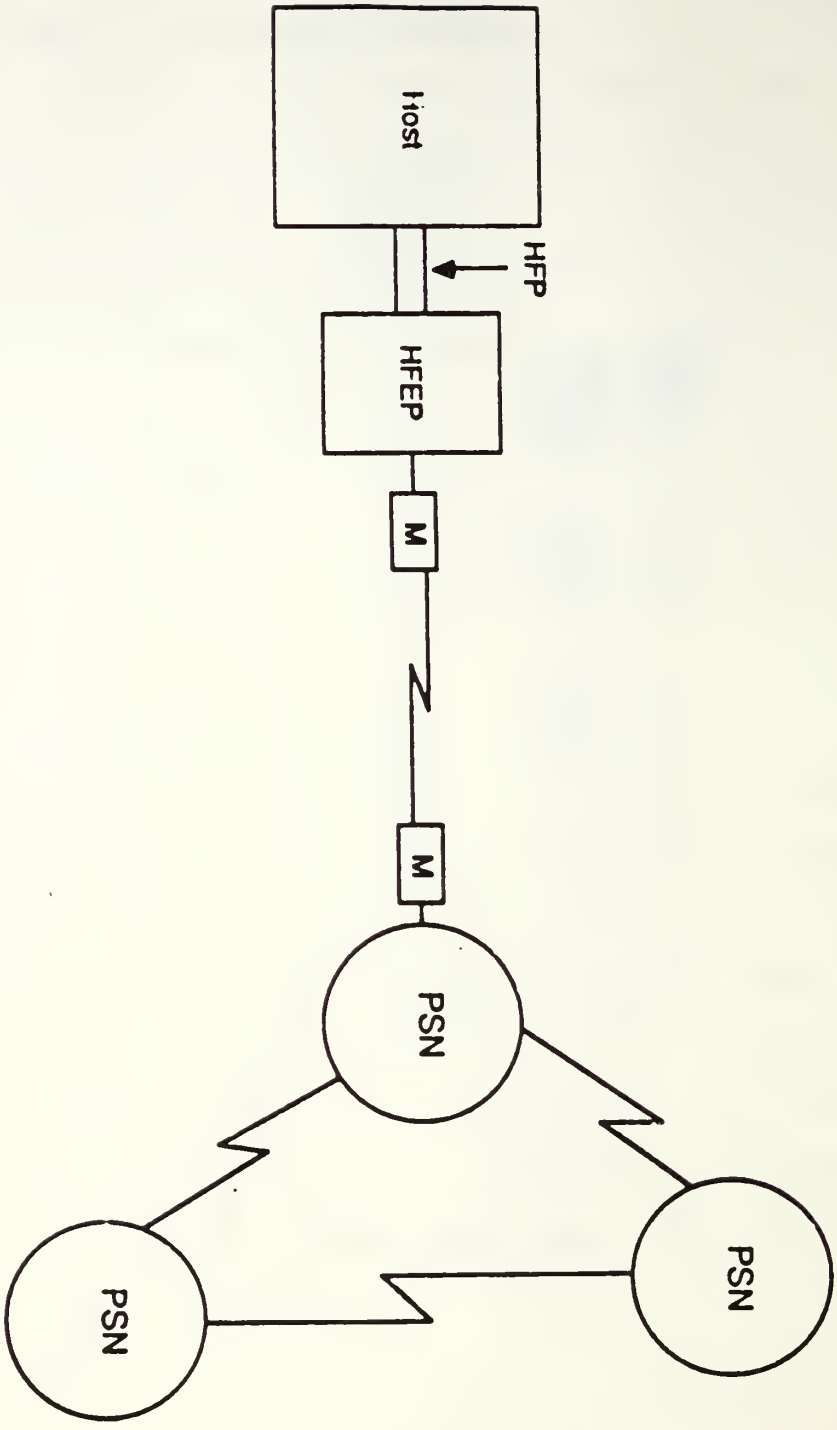

Figure 2.8 Communication Flow Using HFEP.
[from Ref. 5:p. 5-22a]

III. USES OF THE DDN

The primary uses of the DDN are:

1. Electronic mail
2. Virtual terminal access/remote login
3. File transfer.

A subscriber can log into remote computers, transfer files to and from a remote host, and transmit electronic mail messages to and receive messages from users on other hosts via the DDN. Through mail gateways, subscribers can transmit electronic mail messages to users on networks which are not part of the DDN. [Ref. 13:p. 2-4]

A. ELECTRONIC MAIL

Although the original goal of the ARPANET was inter-computer communications, an important benefit has been the DDN's ability to provide electronic mail service. DDN users can compose an electronic message using the composition and editing capability of a mail-supporting computer host usually much like a word processor.

Electronic mail consists of a block of text, complete with source and destination information sent from one DDN user to another. Each network host provides a storage file or mailbox for every user. The supporting host can be accessed locally or remotely through the network. Instead

of utilizing a local host to execute a program or to access its database, a user can generate a file containing a text message at his terminal and then transfer it through the network to a remote host. [Ref. 4:p. 25]

This form of communication has become quite popular in the civilian and military communities as an alternative communications medium to the telephone. Electronic mail supplements the telephone as a cost-effective alternative in the office. Electronic mail also is becoming an integral part of electronic office work stations that provide word processing, database access, files management, and inter-office memo processing, as well as electronic mail. Electronic mail is competitive with the postal service because messages and documents can be transmitted electronically much faster than shipping a letter via the conventional mail service. [Ref. 12:p. 20]

To send a DDN electronic mail message, three items of information are required:

1. User name of the addressee, as assigned by the host.
2. Host name; that is, the official host designation assigned by the DDN.
3. Domain name; that is, the name of the subnetwork on which the host resides (ARPA, EDU, COM, GOV, MIL, etc.).

The information should be supplied in the following general DDN mail address format:

User @ Host.Domain. [Ref. 13:p. 4-10]

This format is based on the DARPA Simple Mail Transfer Protocol (SMTP) which is depicted in Figure 3.1.

1. Infomail

The Defense Communications Agency utilizes the commercial system Infomail (an electronic mail system from Bolt, Beranek, and Newman Communications Corporation) for its electronic mail support on the DDN. The Infomail system provides additional capabilities besides electronic mail. In addition to composition and editing capabilities for generating mail, Infomail can assist in creation of entire documents, and can transmit existing electronic documents (files) between components of the mail host for filing or for transmission to another mailbox. File manipulative capabilities extend from file scans that provide a listing of the source and subject of all mail and documents in the file to specific file searches. [Ref. 12:p. 20]

2. Other Mail Software Packages

In addition to Infomail, various hosts provide different mail support programs. The specific program used is a function of the host computer operating system (UNIX, VMS, TOPS-20, etc.) and of preferences of the host adminstrator. Examples of these include MAIL (UNIX) and MM (TOPS-20).

MAIL is an AT&T Bell Laboratories proprietary operating system that is used to create and manipulate messages on large and small computers. MM is an electronic

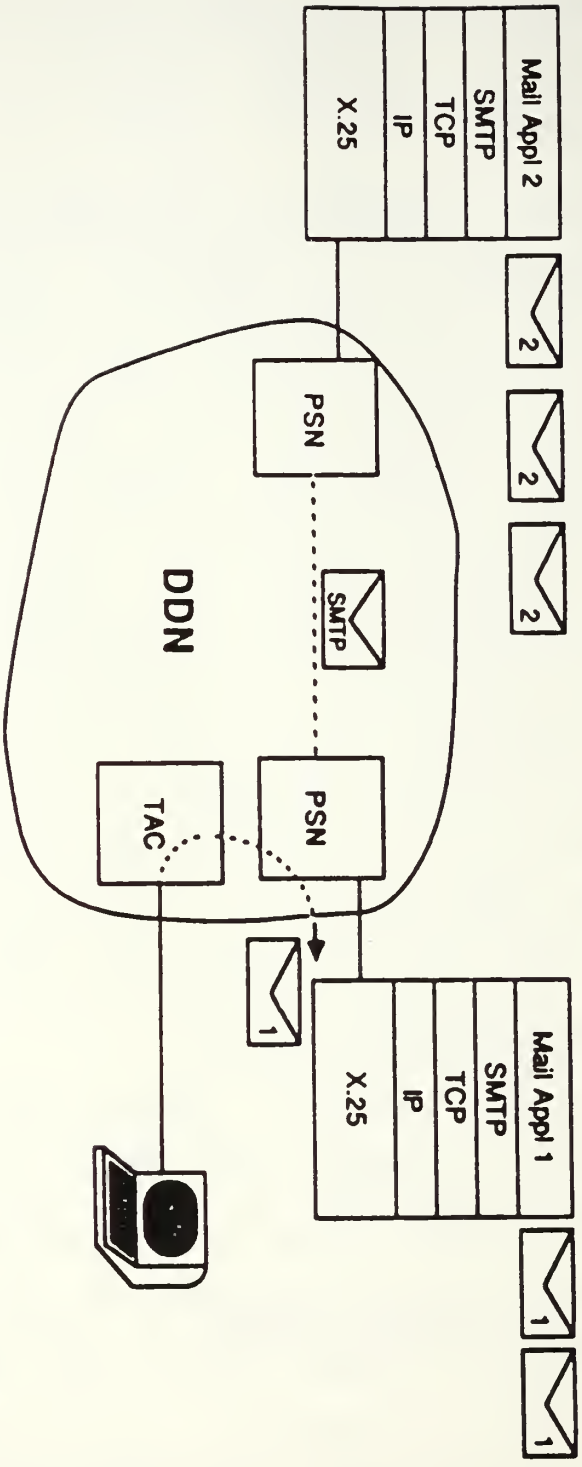

Figure 3.1 Simple Mail Transfer Protocol Configuration. [from Ref. 5:p. 8-25a]

mail handling system used to read messages, to file, store, and retrieve messages, and to send messages to others on MILNET or ARPANET.

B. VIRTUAL TERMINAL ACCESS/REMOTE LOGIN

The DDN allows network subscribers to log in at any host computer on the network for which they are registered users. This feature is referred to as remote login, when the host is not colocated with the user's terminal. The computer at which login initially takes place is referred to as the local host, whereas the computer accessed through the network is known as the remote host. [Ref. 13:p. 5-3]

The process of interfacing a user working at a local terminal or with a remote electronic mail host is usually accomplished with the Telnet application protocol. The Telnet application configuration is depicted in Figure 3.2. Telnet protocol gives the DDN subscriber control over a remote host as if the remote user were a local user of that host. In order to use Telnet the user must have a valid user identification code and password on a local computer as well as on a remote host, and must know the remote computer's official network name or numeric address. Both computers must support the TCP/IP protocol and be connected together by a physical network such as the DDN backbone of PSNs and trunks. [Ref. 13:p. 5-3]

Telnet is available on every fully-capable computer host connected to the DDN. It is fast, reliable, and reasonably

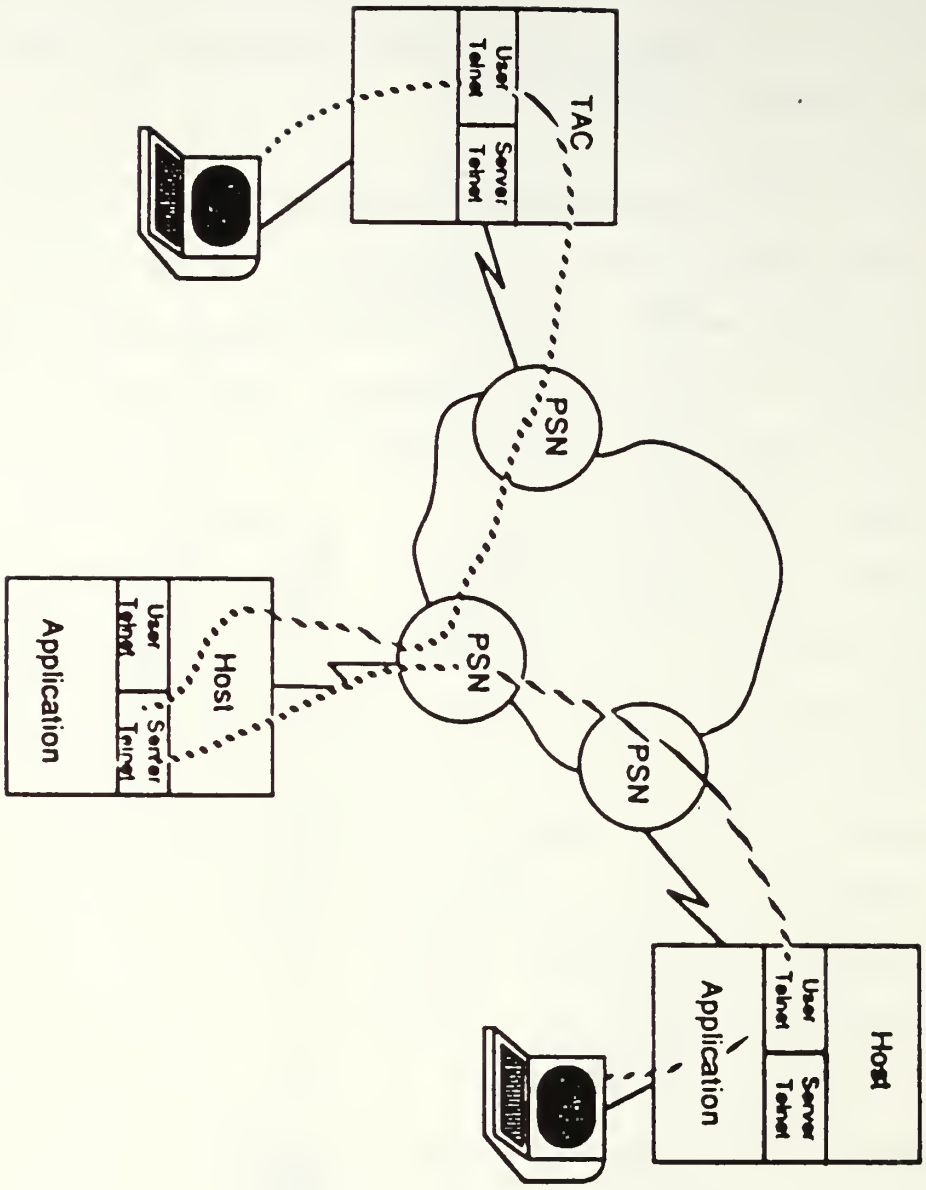

Figure 3.2 Telnet Application Configuration.
[from Ref. 5:p. 8-19a]

user friendly. One major disadvantage of Telnet is that the implementations on different hosts require the user to use different command sets (i.e., Telnet commands used with Computer A may be different from the commands required by Computer B). [Ref. 13:p. 5-4]

Another method of utilizing the DDN's remote login feature is through the use of a TAC. TAC dial-in capability allows the user to connect to a host on the DDN by using a modem-configured terminal to access a TAC, and then ordering the TAC to open a TCP/IP connection to the remote DDN host. One TAC user identification code and password combination is honored by every TAC throughout the world. The user may need to know a remote computer's network name to utilize Telnet, but the user need only know the computer's numeric network address to use a TAC. When travelling, using a TAC is less expensive than placing a long distance phone call to a remote host. Drawbacks to TAC utilization for remote login include:

1. Users are generally confined to low-speed telephone lines.
2. The user must be a registered DDN TAC user. [Ref. 13:p. 5-4]

C. FILE TRANSFER

One of the most important functions of the network is providing the ability to transfer files among the network subscribers. In this application, a file is defined as a block of data that can be addressed and controlled as one

integral unit. A file can be a machine language program or a text of characters. The user's supporting host operating system generally provides the basic file management functions of composing, editing, reading, storing, and discarding files. File transfer is essential for inputting programs on shared computational resources. [Ref. 4:p. 31]

Electronic mail is basically file management with a network transfer capability [Ref. 12:p. 22]. The user generates a file containing the text of the mail through the file compositon capability of either a local or remote network host. The name and address of the receiving user are also included in the text. The file is then transferred via the network to its destination.

The File Transfer Protocol (FTP) application, as illustrated in Figure 3.3, establishes the mechanisms for transmitting files across a network. FTP relies on Telnet to establish the connection between the network hosts prior to the transfer of a file. [Ref. 4:p. 32]

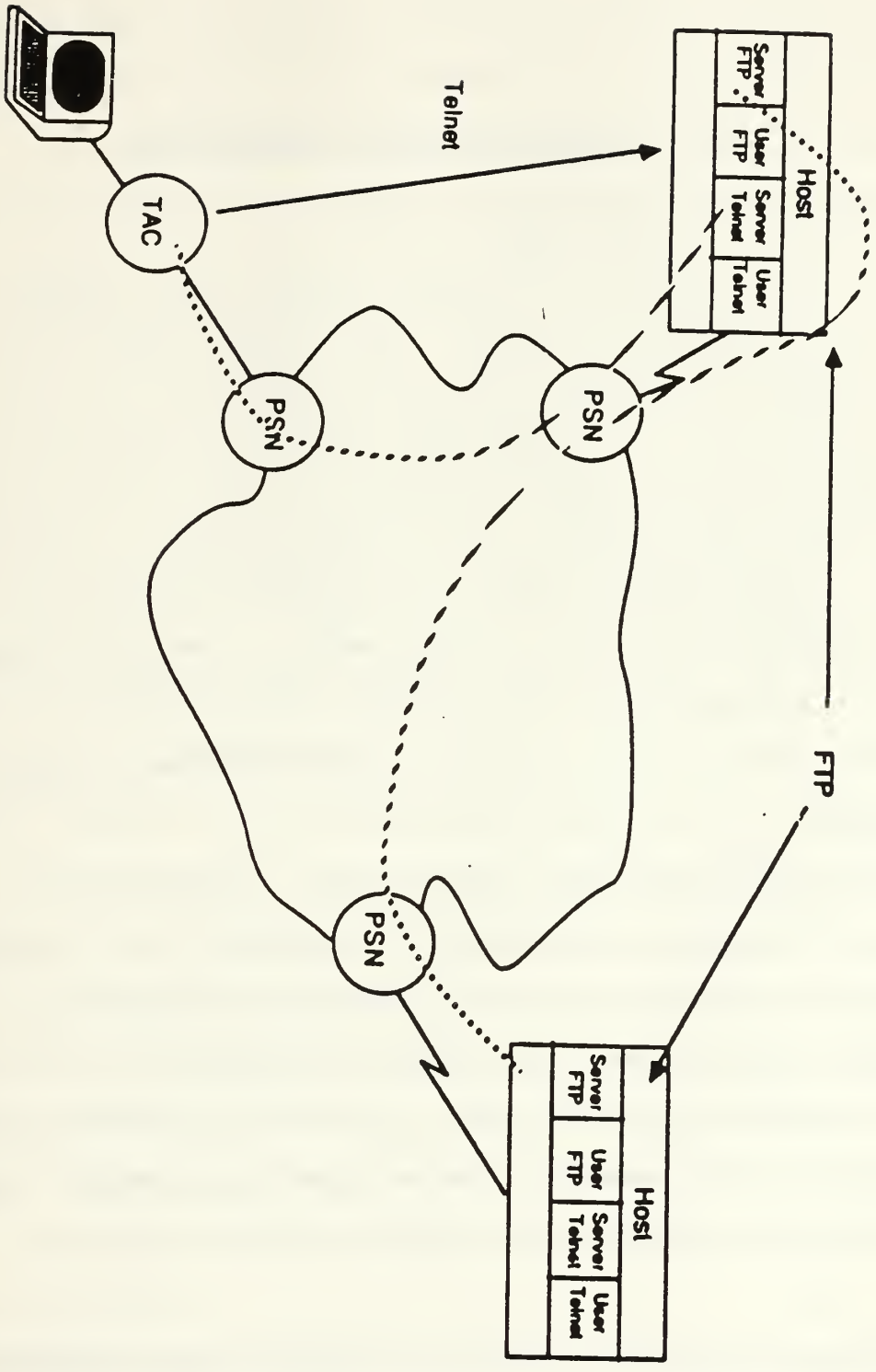

Figure 3.3 File Transfer Protocol Application Configuration. [from Ref. 5:p. 8-22a]

IV. FUTURE DDN CAPACITY AND GROWTH

A. THE DDN USER POPULATION

The DDN provides numerous system applications to a diverse population of users. The Marine Corps is placing its logistics and administrative systems on the network, and the Air Force is upgrading its personnel system for operations using the DDN. The Air Force also is placing its Phase IV Base Supply System on the DDN to provide worldwide coordination among Air Force bases. The Army Inspector General's management information system and the Navy's Regional Data Automation Centers also have been connected to the DDN.

Many organizations use the DDN for electronic mail. Most armed forces management functions (i.e., payroll, logistics, medical records, personnel, intelligence, and command, control, and communication functions) eventually will be maintained on the DDN. The DDN can also be used to communicate data between private firms (contractors) and the governmental agencies for which they are working. [Ref. 14:p. 122]

The multitude of uses for the DDN brings an important question to mind. How large is the potential user population of the DDN?

Approximately 6,000 hosts have been identified as requiring the services of the DDN by the latter part of 1988 [Ref. 2:p. 29]. The DDN program manager estimates that 425 packet switches will be needed by the end of FY89 to service the projected host requirements. [Ref. 15:p. 15.1.4]

The primary reason for promoting a common user data network within the DOD relates to the fact that the larger the DDN becomes the more survivable it is for all subscribers who utilize the network. This scale advantage can be achieved if large numbers of DOD subscriber systems make the transition to the DDN and use the network rather than dedicated communications systems. [Ref. 16:p. 150]

B. CURRENT LIMITS TO GROWTH

The growth of the DDN impacts many of the characteristics of the system. The number of ports on the packet switches must be increased in order to to support attached devices. Additional processor memory is required to maintain the PSN routing tables. New network elements have to be developed to provide cost-effective support for personal computers and synchronous terminals that do not access the DDN through a local area network or private branch exchange.

The ability of the DDN to grow is limited by features of the network's technology. These features can be divided into two categories:

(1) Network software limits

(2) PSN capacity limits. [Ref. 15:p. 15.1.4]

1. Network Software Limits

ARPANET host interface protocol physical-addressing capacity limits the network to 64 hosts per PSN and 256 PSNs per network. The protocol's logical addressing provides for 16,384 host names. The DDN's X.25 protocol allows for 999 packet switches with each switch supporting 99 hosts. If physical addressing is used, the X.25 name space allows for 48,000 logical host names. [Ref. 2:p. 33]

The field sizes which are employed internally in the PSN limit the number of packet switches in a network to 256 and the number of hosts connected to a PSN to 256. Certain features in the PSN software can limit the total number of nodes in a network to 253.

A packet switch contains 256,000 20-bit words of memory. A significant amount of memory is required to support the PSN's routing tables. In the current version of the PSN, 11,000 words are dedicated to logical addressing. This amount of memory is adequate to support about 2,000 host ports if there is an average of two ports per logical name. [Ref. 2:p. 35]

Periodic updates of network usage levels are generated by the PSNs, which measure changes to the network's topology and to the measured delays on network links. The mechanism by which usage updates are performed

requires that each update be carried at least once on every network trunk. As the network grows in size the number of updates received at each packet switch increases as does the amount of processing required for each update. [Ref. 2:p. 37]

2. PSN Capacity Limits

PSN throughput level measures the ability of a PSN to pass data traffic. Throughput is a function of the type of traffic (X.25 or ARPANET host interface protocol), the length of packets, and whether the traffic originates and/or terminates at a host which is local to the PSN. The number of active hosts per PSN is limited on the average to 6.5 by PSN throughput. The maximum capacity of the maximum-size network to absorb traffic is approximately 5.9 megabits per second of user traffic, 9614 host ports, and 1634 simultaneously active hosts. [Ref. 2:p. 43]

C. DDN TECHNOLOGY IMPROVEMENTS

In order to keep pace with the growth of the DDN a series of modifications to the network technology are under development that can improve the ability of the network to expand. The system improvements encompass the areas of:

1. Packet-switch enhancements
2. Network improvements
3. Transmission improvements.

The latest version of the packet switch under development (Release 7) can increase the capacity of each PSN and

the ability of the network to grow. Field sizes will be increased so that a network can support 1024 PSNs, each supporting 256 hosts. Throughput for data traffic entering the network at a given PSN will improve by 60% as a result of software changes in the packet switch. The updated hardware upgrade for the packet switch (C/300) has 512,000 words of memory and can support 64 attached devices (versus the present 44 attached devices). The envisioned capacity of the maximum-sized network with a Release 7 PSN and the C/300 upgrade will include 14,848 host ports, 6465 simultaneously active hosts, and 23 megabits per second of user traffic. [Ref. 2:p. 48]

The DDN program manager is involved in studies to develop techniques to improve network capacity. The focus of these studies is reduction of the amount of routing update information that must be carried on network trunks and processed in network switches. The modified routing procedure will permit the creation of large networks without excessive packet-routing overhead.

A number of developments will facilitate the DDN's ability to obtain additional transmission media to meet the anticipated growth in the amount of network traffic. An example of these developments is the use of the Defense Commercial Telecommunications Network, a bulk lease by DCA of bandwidth from AT&T, that is being incorporated in DDN planning efforts. The DDN also will fund development of the

capability to use switched facilities such as the Public-Switched Telephone Network or dial-up digital services. [Ref. 2:p. 51]

D. FUTURE GROWTH OF THE DDN

The rapid rise in the use of microcomputers and the increasing dependence of military organizations on automated systems will dictate the continued growth of the DDN. Projections of network size in the next five years vary, but the general consensus of the DCA is that several thousand additional host systems will have to be accommodated, serving tens of thousands of terminals. The application of local area networks, the availability of new data transmission services, steady advances in computer security, the use of DOD standard protocols, and the inherent flexibility of the DDN backbone architecture ensure that the increased demands will be met. The DDN undoubtedly will continue serving the defense community through the coming decade and beyond. [Ref. 14:p. 123]

V. FUNDING THE DDN

A. DDN-RELATED COSTS

The principle DDN-related costs are for:

1. Leased communication lines
2. Communications Services Industrial Fund capital investments
3. System engineering and installation
4. Systems operation
5. Life cycle management
6. Network information services. [Ref. 11:p. 11]

The largest cost element for DDN operations is for leased communications lines. DDN capital investments include PSNs, TACs, and network access components. Life cycle management costs represent the second largest component of expenses for the DDN and include the cost of maintaining all network hardware and software. Training services and long-range configuration management also are included in life cycle management costs. Network information services are provided by the NIC, which is funded by the DCA. [Ref. 17:p. 12]

DDN related expenses can be broken down specifically into three areas: common costs, user-specific costs, and traffic-sensitive costs. The DDN Cost Allocation Model uses

a tariff structure that encompasses these three costs. The DDN tariff structure is designed:

1. To provide a basis for the comparison and economic evaluation of various approaches to the utilization of the DDN.
2. To provide the capability to generate sufficient funds to recover network costs.
3. To distribute these costs equitably among network users based on their utilization of the DDN.
4. To promote efficient, cost-effective use of the network.
5. To provide incentives and disincentives designed to reduce users' charges. [Ref. 17:p. 2]

The DDN tariff structure allocates the cost of the DDN on a balanced and equitable basis. The tariff is designed to support cost recovery in such a manner that the amount recovered from each subscriber is proportional to the subscriber's usage of the network's resources [Ref. 11:p. 7].

Common costs can be considered as overhead. The common costs are the basic expenses of providing network services and the expenses of making those services available to the user. User-specific costs refer to those expenses related to providing different types of access for various users (i.e., host access, dedicated terminal access, dial-in terminal access). Traffic-sensitive costs are a function of overall DDN use, and vary with the number of kilopackets (1000 packets) transmitted by the network.

B. INFLUENCE OF DDN DESIGN ON COSTS

The DDN's costs are clearly related to network architecture and design, which strongly influence the following parameters:

1. Network performance requirements.
2. Network reliability requirements.
3. Projected network usage. [Ref. 18:p. 23]

As the number of DDN subscribers increases so does the volume of traffic. Performance standards and requirements related to throughput capacity and delay constraints then define the necessity for additional network assets, such as PSNs and trunk lines, to ensure that data can be moved instantaneously across the network regardless of demand on network resources. To maintain performance standards, continued increases in network capacity thus are necessary, resulting in higher network costs.

Network reliability results in part from the dynamic routing scheme employed by the DDN. Each node has multiple independent connections for enhanced reliability, also increasing DDN expenses.

Network usage is a final factor in the determination of network costs. Network usage characteristics include packet quantities, time of day, geographical distribution of packet travel, duration of use, and type of service. The most important components are packet quantities, that is, average packet length and time-of-day profiles. Total quantity,

duration, and type of service also influence DDN expenses, but to a lesser extent. [Ref. 18:p. 28]

C. DCA COMMUNICATIONS SERVICES INDUSTRIAL FUND

The DDN is currently funded through the Communications Services Industrial Fund (CSIF) managed by DCA. The CSIF charter authorizes DCA to furnish various communications services for DOD:

> Under the management control of the Director, Defense Communications Agency, the purpose of the "Communications Services Activity" is to furnish those communications services, as authorized by the Secretary of Defense, to the Departments and Agencies of the Department of Defense. As directed or authorized by the Director, Defense Communications Agency, or higher authority, the "Communications Services Activity" will also furnish such communications services to other U.S. Government Departments and Agencies or other users as may be appropriate and authorized by law. [Ref. 19:p. 1]

The CSIF charter stipulates that authorized users of the communications services will reimburse the fund according to predetermined subscriber rates approved by the Assistant Secretary of Defense. The subscriber rates include operation and maintenance cost for the backbone network (switches and trunks) and an applicable portion of the operating cost of the Defense Commercial Communications Office. [Ref. 19:p. 2]

Development, acquisition, implementation, operation, and maintenance costs for the DDN are currently shared by DCA, government agencies, and the military departments (MILDEPs). Prior-established CSIF monthly billing rates are paid by the MILDEPs and agencies. The original billing rates were

based on a percentage of the initial requirements identified for each agency or department. In March 1983 the Under Secretary of Defense for Research and Engineering directed that DCA:

> ...develop effective cost recovery alternatives for the DDN through the CSIF based on equitable rates reflecting actual system usage to the maximum extent feasible. [Ref. 3:p. 7]

This directive ensures equitable and efficient cost recovery in light of the projected growth of the DDN and the associated growth of network costs.

Recent DOD budget cuts have forced DOD agencies and the MILDEPs to reexamine their budgets and to prioritize their future expenditures. Federal programs such as the DDN program must be managed as efficiently as possible or they may be cut back substantially or cancelled altogether.

Funding through the CSIF does not promote efficient usage among DDN subscribers. The CSIF's set fee does not take into consideration the fact that abnormally high periods of usage will result in DDN costs being much higher than the predetermined rate. This situation results in a disparity between the costs incurred by usage and the funds received in payment from the DDN's subscriber.

D. USAGE SENSITIVE BILLING

The DDN program plan approved by the Deputy Secretary of Defense on 2 April 1982 [Ref. 20] and subsequent policy guidance provide for the eventual recovery of the DDN's

network costs by billing subscribers based upon their utilization of network resources. This practice is termed Usage Sensitive Billing (USB) and is designed:

1. To ensure that sufficient funds are generated to recover CSIF-funded network cost.
2. To distribute network costs equitably among network users based on their utilization of the network.
3. To reduce network costs by promoting efficient, cost-effective use of the network.
4. To provide cost incentives to the user for optimum utilization of network resources. [Ref. 20]

The Office of the Joint Chiefs of Staff has directed that USB be implemented by each service no later than FY90. To comply with this decree DCA has published FY90 CSIF rates for the DDN. Table IV illustrates how these rates are calculated. [Ref. 20]

Usage Sensitive Billing will enable the DDN program manager to exert more control over the utilization of the network. Each DDN subscriber will be charged appropriately for their individual usage, thus providing users with an incentive to keep operating costs down. The cost-efficient utilization of the DDN can help maintain the program's viability during this tumultuous period of scarce fiscal resources. In order to survive the DOD budget cuts, the DDN program must be self-sufficient. USB ensures that subscribers which utilize few DDN resources do not subsidize subscribers which utilize vast DDN resources.

TABLE IV

DEFENSE DATA NETWORK USAGE SENSITIVE BILLING WORKSHEET
TO COMPUTE MONTHLY CHARGES
[From Ref. 20]

Connections	Quantity		Monthly Charge		TOTAL Monthly Cost
Host - Single					
9.6 KB or less	_____	@	$1,750	=	_____
over 9.6 KB	_____	@	$4,000	=	_____
Host - Dual Homed					
9.6 KB or less	_____	@	$2,700	=	_____
over 9.6 KB	_____	@	$6,500	=	_____
Terminal	_____	@	$ 450	=	_____
Dial-In Access	_____		hours @ $4.50/hr	=	_____

Usage

Usage charges are based on kilopackets at peak and off-peak hours and by precedence level used. Currently, only one precedence level is available. The peak hour charge is $1.25 per kilopacket. Off-peak hour charge is currently $.60 per kilopacket. For FY90 it is expected to be increased to $.90 per kilopacket.

Until enough actual usage data for your system is collected, recommend you use the following estimations. These estimates are averages obtained from sampling actual usage of an operational Navy activity.

	AVERAGE	HIGHEST USER (ONLY ONE IN SAMPLE)
9.6 KB or less	$10K/month	$54K/month
over 9.6 KB	$41K/month	$120K/month

The fact must be established that DDN costs incurred and how the billing process recovers these costs are two separate issues. The initial expenditures for the DDN include the engineering and planning costs, hardware and software implementation costs, and trunk acquisition costs. Once a network is operational, however, these expenditures become sunk/fixed costs. The CSIF fixed-rate fee can recover the fixed costs, but is insufficient to cover the growth of the network. As more and more DDN subscribers utilize the system, network costs rise substantially. A traffic-sensitive scheme such as USB is needed to cover the costs of an expanding system adequately.

VI. DON'S DDN PROGRAM

A. DON'S DDN IMPLEMENTATION PLAN

The objectives of the Navy's DDN implementation program are:

1. To provide DON system subscribers with improved data communications capability
2. To provide DON system subscribers with a highly survivable and reliable means of connection with other DDN users
3. To reduce overall DON telecommunications costs. [Ref. 21:p. 4]

1. Procedure For Connecting DON Systems to the DDN

Potential Navy host subscribers have three options by which to connect to the DDN. The first option requires the development of modifications to the host system software to conform with DDN software communication protocols. The second option allows for the use of a HFEP to support the X.25 and TCP/IP protocols. The third option involves the TEP. The TEP's limited interoperability, however, precludes it from being a recommended DDN interface for Navy systems. [Ref. 21:p. 4]

The initial step for subscriber connection to the DDN is submission of information concerning the host system and terminals to the Commander, Naval Telecommunications Command (COMNAVTELCOM), for inclusion in DCA's user requirements data base (URDB). The URDB submission provides

technical and operational requirements information that is used by the DCA for network configuration planning and connection scheduling. The potential subscriber is responsible for selecting the type of interface that will be used for connection to the DDN. Factors that should be considered are:

1. The present and projected requirements for interoperability with other Navy or DOD systems
2. The availability of a developed interface in the host vendor's product line
3. The computational resources available within the host system. [Ref. 21:p. 22]

Upon approval of the potential subscriber's interface approach, a site visit is conducted by technical representatives of the DCA. The reasons for the site visit are:

1. To verify technical characteristics of the candidate subscriber system
2. To review installation space characteristics if a DDN node or TAC is required
3. To resolve outstanding technical or managerial issues. [Ref. 21:p. 25]

Based on discussions and agreements obtained during the site visit, the candidate subscriber prepares an Installation and Implementation Plan. This plan contains schedule information, required facilities modifications, logistic support plans, and operational requirements. The installation plan is the primary guidance document for candidate subscriber cutover planning.

A Request for Service document is required to acquire common carrier communication lines from the DCA. This request contains detailed technical information concerning circuits required, locations of all services required, and a schedule for the start of services. Upon validation of the request a telecommunications service request is forwarded to the DCA for issuance of a telecommunications service order to acquire the necessary circuits. Upon completion of the system testing process the subscriber notifies the Defense Communications System Circuit Control Office of circuit activations. These reports provide the information necessary to maintain billing records for leased circuits and equipment. [Ref. 21:pp. 26-28]

2. DON Connection Schedule Planning Considerations

In developing the Navy's implementation schedule for the DDN system, COMNAVTELCOM incorporated the following factors to establish the priority and schedule for system connection:

1. The cost benefit accruing to the Navy for each system proposed for connection to the DDN
2. The subscriber's operational requirements for improved connectivity, reliability, and survivability
3. The availability of a means to interface the system to the DDN
4. The individual development schedule
5. The availability of cryptographic devices. [Ref. 21:p. 36]

Many Navy systems are in the process of cutover onto the MILNET and the DISNET. Major commands have taken the advent of the DDN as an opportunity to restructure their ADP/communications to gain maximum benefits in improved data communications capability, along with lower costs. The availability of DDN-qualified interfaces has increased and is growing steadily. The cutover schedule for the classified systems to the DISNET will be worked concurrently with the unclassified network. [Ref. 21:p. 38]

B. MANAGEMENT OF THE NAVY'S DDN PROGRAM

1. Management Responsibilities

The Chief of Naval Operations (OP-941) has assigned COMNAVTELCOM to overall project coordination of the Navy's DDN program. COMNAVTELCOM coordinates directly with individual commands for tactical systems and with the Commander, Naval Data Automation Center, for specific non-tactical systems. The Naval Telecommunications Automation Support Center provides technical assistance in support of the analysis and implementation of the Navy's DDN program. The Director, Command and Control (OP-094), is tasked as the Navy's DDN program sponsor. The Director, Naval Communications Division (OP-941), exercises program coordinator responsibilities for OP-094. [Ref. 21:p. B-2]

2. Logistics Responsibilities

The DCA is the procurement agency for DDN equipment and standard software. The MILDEPs and agencies obtain DDN

access equipment through their normal communication acquisition organizations. Each subscriber must develop or procure DDN interfaces individually. The DCA is updated on individual subscriber needs through the subscriber's inputs to its URDB.

Network maintenance is handled on a contractual basis by the DCA. DON subscribers are responsible for the maintenance of their hardware interface equipment and network access software. [Ref. 21:pp. 32-33]

C. AN ASSESSMENT OF THE NAVY'S DDN PROGRAM

1. State of the Program

The DDN has evolved into a major, robust program. Unfortunately network-subscriber requirements have grown at the same time that the DCA has been experiencing system connection delays. The growing use of personal computers has intensified this problem. [Ref. 22:p. 7] Systems with complex interfaces and high data transfer requirements are experiencing difficulty transitioning to the DDN [Ref. 23:p. 11]

However, recognition of these concerns has prompted the DCA to improve support for DON subscribers of the DDN. This support has materialized in the form of DCA initiatives:

1. To form "tiger teams" (teams of personnel that are experts on the DDN) and task forces to improve the implementation and installation of DDN equipment at Navy sites.

2. To institute work order revisions to define user requirements for the URDB more concisely.

3. To promote better administrative and technical DDN coordination from the Naval Telecommunications Automation Support Center.

4. To ensure that the Naval Data Automation Center provides planning support for DON information systems using the DDN. [Ref. 23:p. 10]

As a result of this increased attention, the major areas of concern seem to be moving from a lack of interface software to the integration of DDN software and the operational performance of the network. The Navy still must prioritize its DDN requirements and ensure that the DCA is kept appraised of all present and emergent problem areas. Although guidelines for network interoperability and architectures for data communications are being developed, the DCA will not be able to meet all the Navy's projected requirements. As a result, the DON must do the following:

1. Find interim ways to concentrate host connections.

2. Develop alternate means to transmit bulk data.

3. Study the use of standard protocols. [Ref. 23:p. 12]

Currently the DDN is centrally funded within the DON. The Commander, Naval Telecommunications Command, provides a fixed monthly payment to the CSIF. DON will implement USB in FY90. Procedures to implement USB throughout DON are designed to relate DDN costs directly to various activities' usage of the network. Charges, based on usage, will be billed to each user activity by the DCA beginning in FY90. This will provide an incentive to the

DON activities to use the network in an efficient manner. [Ref. 20]

2. Problem Areas

The rapid growth of the DDN has resulted in the system's requirements exceeding the network's available connection capability. This problem can be attributed to two factors:

1. AT&T divestiture has greatly complicated implementation procedures and extended lead times associated with the acquisition of trunk lines.
2. The DDN transition schedule (from the initial URDB submission to actual live connection to the DDN) takes approximately two years to complete. [Ref. 22:p. 6]

The spread of informal (versus formal) electronic mail service on the DDN is an established trend. Although this communication method is eagerly sought by individual users, electronic mail service does not always receive dedicated support at the command level. Unless properly implemented, electronic mail service can become fragmented and place an excessive traffic load on the network. [Ref. 22:p. 6]

The future of the DDN as a multi-level secure network depends on the success of the BLACKER program. The failure of the BLACKER program would have an adverse effect on the Navy's DDN program because some DON systems require interoperability with systems operating at different security levels. [Ref. 23:p. 9]

The Navy's DDN implementation plan poses growth problems. Earlier estimates defining user requirements were inaccurate. How large demand for DDN services will ultimately become is uncertain. The existing capability to install new equipment and acquire new trunks is not adequate. The need for qualified interface software continues to grow and synchronous terminal support is still a problem. [Ref. 22:p. 7]

The DDN's constant growth and changing technology have resulted in frustration and confusion among many DON users. The lack of an organized training environment for the DDN forces most new users to rely on on-the-job training to become proficient DDN users. The constant rotation of personnel intensifies this problem. By the time DDN users become proficient they are retired, discharged from the Navy, or transferred to a new duty assignment. Their place on the DDN learning curve is usually not passed on to the person relieving them; as a result, the command loses access to a valuable asset. The confusion and frustration continues because there is little, if any, organized information exchange throughout the Navy concerning the DDN.

The recent DOD/DON budget cuts enacted by Congress present a formidable challenge to the future expansion of the DDN. Reduced funding of the DDN program will seriously impact the implementation and installation of new DON systems. Future enhancements of the network's technology

undoubtably will be jeopardized by limited expenditures for research and development.

3. Benefits for Navy Systems

Connection to the DDN will provide several benefits to DON subscribers. These benefits include:

1. Improved interoperability with other DDN systems via the implementation of appropriate DDN software protocols
2. Improved survivability via dual homing and adaptive-routing techniques
3. Reduction in subscriber circuit mileage costs via a high-capacity, efficient, common user network
4. Reduction in network control facilities via NMCs that have the responsibility for monitoring and trouble-shooting all network access links and backbone trunks. [Ref. 21:p. 5]

The DDN's improved interoperability will enable the DON to interface with other MILDEPs and DOD agencies that are connected to the network. DDN equipment used for communication (i.e., TACs, PSNs) is compatible throughout the DOD. The improved survivability feature of the DDN enables DON subscribers to interact with other DOD subscribers during high-stress periods or crisis situations--when other systems tend to malfunction.

The common user, high data capacity feature of the DDN will reduce the DON's communications costs. The use of public transmission media and the network's high data throughput make the system a cost-efficient program for DON subscribers. USB will promote more efficient usage of the

network, therefore, enabling DON subscribers to reduce their communications costs.

The NMCs provide centralized management and administrative support for the DDN. DON subscribers can easily access the cognizant NMC whenever network-related problems arise. This feature also facilitates ease of operation, reduced complexity, and rapid recovery from emergency conditions (i.e., natural disasters, sabotage, equipment failure).

VII. CONCLUSIONS AND RECOMMENDATIONS

A. CONCLUSIONS

The focal point of this thesis has been to analyze the Navy's DDN program. As noted, the DDN provides high quality, reliable, survivable data communications service today and will provide increasingly survivable service in the future, as its user and asset base expands [Ref. 16:p. 158].

The DDN offers DON subscribers several features that are a vast improvement over the forms of communication presently used (i.e., telephone, Naval message and speedletter, interoffice and intraoffice memos). The electronic mail, Telnet, and file transfer features of the DDN would enable the Navy to diminish its dependence on message traffic by transferring data via electronic means. DDN technology adheres to the basic requirements that all military networks must meet: worldwide survivability, security, performance, and responsiveness. The DDN also provides reduced subscriber mileage costs and streamlined network control facilities.

Although the DDN has the potential to become an invaluable asset to the DON's communication system, until now there has been very little impact by the DDN on communications Navy-wide. The DON has resisted discarding

the traditional methods of communication utilized in the Navy. Only a few Naval commands (e.g., the Naval Data Automation Center, Naval Ocean Systems Center) have made a dedicated effort to transition fully into the DDN.

There is hope, however, for the Navy's DDN program. Many of the problems noted here have been identified and addressed by COMNAVTELCOM and the DCA. Guidelines on interoperability and architectures for data communications are being established. DON is prioritizing its projected requirements to ensure that the DDN meets the majority of the Navy's communication needs in the future. The DCA's initiatives to improve the Navy's DDN program (i.e., tiger teams, URDB updates, work order revisions) should alleviate many problem areas.

B. RECOMMENDATIONS

In order to improve the DDN's acceptability among DON subscribers and to avoid unnecessary problems in the future, more command-level attention must be focused on the Navy's DDN program. Command-level attention (Navy captain and above) is essential to implement the transition from the Navy's traditional methods of communication to the high-tech capability of the DDN.

The transition requires a change strategy. DON personnel must be formally trained to use the DDN and to overcome the inherent reluctance to use a new system. An organized training program must be instituted Navy-wide to

indoctrinate DON personnel properly about the DDN's capabilities.

COMNAVTELCOM should ensure that there is continuous interaction and dialogue between established DON DDN subscribers and potential subscribers. Better coordination and feedback between the various Naval commands will ultimately enhance the DON's utilization of the DDN.

APPENDIX

Abbreviations and Acronyms

ADP	Automatic Data Processing
ARPANET	Advanced Research Project Agency Network
BBN	Bolt, Beranek, and Newman
BER	Bit Error Rate
BFE	Blacker Front End
BPS	Bits per second
COMNAVTELCOM	Commander, Naval Telecommunications Command
CRT	Cathode Ray Tube
CSIF	Communication Services Industrial Fund
DARPA	Defense Advanced Research Projects Agency
DCA	Defense Communications Agency
DDN	Defense Data Network
DOD	Department of Defense
DON	Department of the Navy
EGP	Exterior Gateway Protocol
FTP	File Transfer Protocol
GGP	Gateway-to-Gateway Protocol
HDH	High-level Data Link Control Distant Host
HDLC	High-level Data Link Control
HFEP	Host Front End Protocol

ICMP	Internet Control Message Protocol
IMP	Interface Message Processor
IP	Internet Protocol
IPLI	Internet Private Line Interface
JCS	Joint Chiefs of Staff
MC	Monitoring Center
MILDEP	Military Department
MILNET	Military Network
MINET	Movement Information Network
NIC	Network Information Center
NMC	Network Monitoring Center
PSN	Packet-Switching Node
SACDIN	Strategic Air Command Digital Network
SATNET	Satellite Network
SCINET	Sensitive Compartmented Information Network
SMTP	Simple Mail Transfer Protocol
TAC	Terminal Access Controller
TCP	Transmission Control Protocol
TEP	Terminal Emulation Processor
ULP	Upper Level Protocol
URDB	User Requirements Data Base
USB	Usage Sensitive Billing
WIN	WWMCCS Intercomputer Network
WWMCCS	World Wide Military Command and Control System

LIST OF REFERENCES

1. Hurlburt, John H., "Defense Data Network Status: A Vendor Perspective," Government Executive, January 1986.

2. Defense Communications Agency, The Defense Data Network, Washington, D.C., 1986.

3. The Under Secretary of Defense, Research and Engineering, Defense Data Network (DDN) Implementation, 10 March 1983.

4. Department of Defense, Defense Communications Agency, Defense Data Network System Description, January 1984

5. Department of Defense, Defense Communications Agency, The DDN Course, April 1986.

6. Rosner, Roy D., Packet Switching, Lifetime Learning Publications, 1984.

7. Heggestad, Harold M., "An Overview of Packet-Switching Communications," IEEE Communications, v. 22, p. 24, April 1984.

8. Hagouel, Jacob, "Source Routing and a Distributed Algorithm to Implement It," IEEE INFOCOM 1983, IEEE Computer Society Press, 1983.

9. Caldwell, M., Improvements in Routing for Packet Switched Networks, Ph.D. Dissertation, George Washington University, Washington, D.C., 1975.

10. Perlman, R., "Fault Tolerant Broadcast Information," IEEE INFOCOM 1983, IEEE Computer Society Press, 1983.

11. Defense Communications Engineering Center, Specific Recommendations for Improving Network Feedback to Host, 1985.

12. Kavanaugh, Kevin R., Efficiency Analysis of the Electronic Mail System (INFOMAIL) On the Defense Data Network, Master's Thesis, Air Force Institute of Technology, Wright-Patterson Air Force Base, Ohio, December 1984.

13. Naval Ocean Systems Center Technical Document 940, Introduction to the Defense Data Network (DDN), by C. T. Messinger, January 1986.

14. Elsam, Eric S., "The Defense Data Network Hits Its Stride," Telecommunications, v. 20, pp. 121-123, May 1986.

15. Maybaum, F. Lee, Colonel, USAF, "Defense Data Network: An Overview," IEEE, pp. 15.1.1-15.1.6, 1986.

16. Fidelman, Miles R., "Survivability of the Defense Data Network," Signal, pp. 148-158, May 1986.

17. Department of Defense, Defense Communications Agency, DDN Cost Allocation Model, September 1984.

18. McNamara, Kathryn, Defense Data Network: Usage Sensitive Billing, Master's Thesis, Naval Postgraduate School, Monterey, California, June 1986.

19. Department of Defense, Defense Communications Agency, Defense Industrial Fund Charter for Financing Operations of the "Communications Services Industrial Fund" Activity of the Defense Communications Agency, April 1975.

20. Chief of Naval Operations (CNO), Usage Sensitive Billing, Message 012070Z, October 1987.

21. Department of Defense, Commander Naval Telecommunications Command, Navy Planning Guidance For Defense Data Network Implementation, October 1986.

22. Office of the Under Secretary of Defense for Research and Engineering, Defense Science Board Task Force on Defense Data Network Final Report, pp. 6-14, 30 August 1985.

23. Department of Defense, Commander Naval Telecommunications Command, Navy's DDN Program: An Assessment, October 1987.

INITIAL DISTRIBUTION LIST

		No. Copies
1.	Defense Technical Information Center Cameron Station Alexandria, Virginia 22304-6145	2
2.	Library, Code 0142 Naval Postgraduate School Monterey, California 93943-5002	2
3.	Professor Judith Lind, Code 55Li Naval Postgraduate School Monterey, California 93943-5002	2
4.	Professor Gary Poock, Code 55Pk Naval Postgraduate School Monterey, California 93943-5002	1
5.	Professor Dan C. Boger, Code 54Bo Naval Postgraduate School Monterey, California 93943-5002	2
6.	Director, Naval Communications OP-941 Pentagon, Room 5A718 Washington, DC 20350	1
7.	Lt. Victor B. Stuckey 409 East Mary Street Dublin, Georgia 31021	5
8.	Mrs. Margaret Campbell 377-C Bergin Drive Monterey, California 93940	1